ProCurve Series 6120 Switches

Advanced Traffic Management Guide

August 2009

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. All Rights Reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5992-5524
August 2009

Applicable Products

HP ProCurve Switch 6120G/XG	(498358-B21)
HP ProCurve Switch 6120XG	(516733-B21)

Trademark Credits

Microsoft, Windows, and Microsoft Windows NT are US registered trademarks of Microsoft Corporation.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty information at **http://www.hp.com/#Support.**

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

HP Contact Information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage **(http://welcome.hp.com/country/us/en/wwcontact.html).**

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage **(http://welcome.hp.com/country/us/en/contact_us.html)**. To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (**http://www.hp.com/hps**).
- In other locations, see the Contact HP worldwide (in English) webpage **(http://welcome.hp.com/country/us/en/wwcontact.html**).

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.procurve.com

Contents

Product Documentation

About Your Switch Manual Set ix

Printed Publications. ix

Electronic Publications ix

Software Feature Index. x

1 Getting Started

Contents 1-1

Introduction 1-2

Conventions 1-2

Command Syntax Statements 1-2

Command Prompts 1-3

Screen Simulations 1-3

Configuration and Operation Examples 1-3

Keys 1-3

Sources for More Information 1-4

Getting Documentation From the Web 1-6

Online Help 1-6

Menu Interface 1-6

Command Line Interface 1-7

Web Browser Interface 1-7

Need Only a Quick Start? 1-8

IP Addressing 1-8

To Set Up and Install the Switch in Your Network 1-8

Physical Installation 1-8

2 Static Virtual LANs (VLANs)

Contents 2-1

Overview 2-3

Introduction 2-4
General VLAN Operation 2-4
Types of Static VLANs Available in the Switch 2-5
Port-Based VLANs 2-5
Protocol-Based VLANs 2-5
Designated VLANs 2-5
Terminology 2-6
Static VLAN Operation 2-7
VLAN Environments 2-8
VLAN Operation 2-9
Overlapping (Tagged) VLANs 2-10
Per-Port Static VLAN Configuration Options 2-12
VLAN Operating Rules 2-13
General Steps for Using VLANs 2-16
Multiple VLAN Considerations 2-17
Single Forwarding Database Operation 2-17
Example of an Unsupported Configuration and How To Correct It 2-19
Multiple Forwarding Database Operation 2-20
Configuring VLANs 2-21
Menu: Configuring Port-Based VLAN Parameters 2-21
To Change VLAN Support Settings 2-22
Adding or Editing VLAN Names 2-23
Adding or Changing a VLAN Port Assignment 2-25
CLI: Configuring Port-Based and Protocol-Based VLAN Parameters 2-27
Web: Viewing and Configuring VLAN Parameters 2-39
802.1Q VLAN Tagging 2-40
Special VLAN Types 2-45
VLAN Support and the Default VLAN 2-45
The Primary VLAN 2-45
The Secure Management VLAN 2-46
Preparation 2-48
Configuration 2-49
. 2-49
Using DHCP to Obtain an IP Address 2-50

Deleting the Management VLAN 2-53
Operating Notes for Management VLANs 2-53
Voice VLANs 2-54
Operating Rules for Voice VLANs 2-54
Components of Voice VLAN Operation 2-55
Voice VLAN Access Security 2-55
Effect of VLANs on Other Switch Features 2-55
Spanning Tree Operation with VLANs 2-55
IP Interfaces 2-56
VLAN MAC Address 2-56
Port Trunks 2-56
Port Monitoring 2-56
Jumbo Packet Support 2-57
VLAN Restrictions 2-57

3 GVRP

Contents 3-1
Overview 3-2
Introduction 3-3
General Operation 3-4
Per-Port Options for Handling GVRP "Unknown VLANs" 3-7
Per-Port Options for Dynamic VLAN Advertising and Joining 3-9
GVRP and VLAN Access Control 3-11
Advertisements and Dynamic Joins 3-11
Port-Leave From a Dynamic VLAN 3-11
Planning for GVRP Operation 3-12
Configuring GVRP On a Switch 3-13
Menu: Viewing and Configuring GVRP 3-13
CLI: Viewing and Configuring GVRP 3-14
Web: Viewing and Configuring GVRP 3-18
GVRP Operating Notes 3-18

4 Multiple Instance Spanning-Tree Operation

Contents 4-1

Overview 4-3

802.1s Multiple Spanning Tree Protocol (MSTP) 4-6

MSTP Structure 4-7

How MSTP Operates 4-9

MST Regions 4-9

Regions, Legacy STP and RSTP Switches, and the Common Spanning Tree (CST) 4-11

MSTP Operation with 802.1Q VLANs 4-12

Terminology 4-13

Operating Rules 4-15

MSTP Compatibility with RSTP or STP 4-16

Configuring MSTP 4-17

Planning an MSTP Application 4-17

MSTP Configuration Overview 4-19

Configuring MSTP Operation Mode and Global Settings 4-21

Configuring MSTP Per-Port Parameters 4-26

Configuring Per Port Parameters 4-26

Configuring BPDU Filtering 4-30

Configuring BPDU Protection 4-31

Configuring MST Instance Parameters 4-35

Configuring MST Instance Per-Port Parameters 4-37

Enabling or Disabling Spanning Tree Operation 4-40

Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another 4-40

MSTP VLAN Configuration Enhancement 4-42

PreConfiguring VLANs in an MST Instance 4-43

Configuring MSTP Instances with the VLAN Range Option 4-44

Operating Notes for the VLAN Configuration Enhancement . . . 4-46

How to Save Your Current Configuration 4-47

Displaying MSTP Statistics and Configuration 4-49

Displaying Global MSTP Status 4-50

Displaying Detailed Port Information 4-52

Displaying Status for a Specific MST Instance 4-53

Displaying the MSTP Configuration 4-54
Troubleshooting an MSTP Configuration 4-58
Displaying the Change History of Root Bridges 4-58
Displaying Debug Counters for All MST Instances 4-61
Displaying Debug Counters for One MST Instance 4-62
Displaying Debug Counters for Ports in an MST Instance 4-64
Field Descriptions in MSTP Debug Command Output 4-66
Troubleshooting MSTP Operation 4-69
Loop Protection 4-70
Configuring Loop Protection 4-71
Viewing Loop Protection Status 4-72

5 Quality of Service (QoS): Managing Bandwidth More Effectively

Contents 5-1
Introduction 5-3
Terminology 5-6
Overview 5-7
Classifiers for Prioritizing Outbound Packets 5-10
Packet Classifiers and Evaluation Order 5-10
Preparation for Configuring QoS 5-11
Preserving 802.1p Priority 5-11
Steps for Configuring QoS on the Switch 5-11
Viewing the QoS Configuration 5-13
No Override 5-13
Using QoS Classifiers to Configure Quality of Service for Outbound Traffic 5-14
QoS IP Type-of-Service (ToS) Policy and Priority 5-15
Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits 5-16
Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP 5-17
Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices 5-21
Details of QoS IP Type-of-Service 5-24

QoS Source-Port Priority 5-27
Assigning a Priority Based on Source-Port 5-27
Assigning a DSCP Policy Based on the Source-Port 5-29
Differentiated Services Codepoint (DSCP) Mapping 5-33
Default Priority Settings for Selected Codepoints 5-34
Quickly Listing Non-Default Codepoint Settings 5-34
Notes on Changing a Priority Setting 5-36
Error Messages caused by DSCP Policy Changes 5-36
Example of Changing the Priority Setting on a Policy When One or More Classifiers Are Currently Using the Policy . 5-37
QoS Queue Configuration 5-40
QoS Operating Notes and Restrictions 5-41
IP Multicast (IGMP) Interaction with QoS 5-43

Product Documentation

About Your Switch Manual Set

Note

For the latest version of switch documentation, please visit any of the following websites:

www.procurve.com/manuals

www.hp.com/go/bladesystem/documentation

h18004.www1.hp.com/products/blades/components/c-class-tech-installing.html

Printed Publications

The publication listed below is printed and shipped with your switch. The latest version is also available in PDF format, as described in the Note at the top of this page.

- *Quick Installation Card*—Explains how to prepare for and perform the physical installation and connect the switch to your network.

Electronic Publications

The latest version of each of the publications listed below is available in PDF format on the ProCurve Web site, as described in the Note at the top of this page.

- *Installation and Getting Started Guide*—Describes how to install hardware, and get started using the switch.
- *Management and Configuration Guide—Describes how to configure, manage, and monitor basic switch operation.*
- *Advanced Traffic Management Guide*—Explains how to configure traffic management features such as VLANs, MSTP, and QoS.
- *Multicast and Routing Guide*—Explains how to configure IGMP features.
- *Access Security Guide*—Explains how to configure access security features and user authentication on the switch.
- *IPv6 Configuration Guide*—Describes the IPv6 protocol operations that are supported on the switch.
- *Release Notes*—Describe new features, fixes, and enhancements that become available between revisions of the main product guide.

Software Feature Index

This feature index indicates which manual to consult for information on a given software feature.

Note

This Index does not cover IPv6 capable software features. For information on IPv6 protocol operations and features (such as DHCPv6, DNS for IPv6, and Ping6), refer to the *IPv6 Configuration Guide*.

Intelligent Edge Software Features. These features are automatically included on all switches.

Intelligent Edge Software Features	Manual			
	Management and Configuration	Advanced Traffic Management	Multicast and Routing	Access Security Guide
802.1Q VLAN Tagging		X		
802.1X Multiple Authenticated Clients Per Port				X
AAA Authentication				X
Authorized IP Managers				X
Authorized Manager List (Web, Telnet, TFTP)				X
Auto MDIX Configuration	X			
BOOTP	X			
Config File	X			
Console Access	X			
Copy Command	X			
CoS (Class of Service)		X		
Debug	X			
DHCP Configuration	X			
DHCP/Bootp Operation	X			
Diagnostic Tools	X			

Intelligent Edge Software Features	Manual			
	Management and Configuration	Advanced Traffic Management	Multicast and Routing	Access Security Guide
Downloading Software	X			
Event Log	X			
Factory Default Settings	X			
Flow Control (802.3x)	X			
File Transfers	X			
Friendly Port Names	X			
GVRP		X		
Identity-Driven Management (IDM)		X		
IGMP			X	
Interface Access (Telnet, Console/Serial, Web)	X			
IP Addressing	X			
Jumbo Packets	X			
LACP	X			
LLDP	X			
LLDP-MED	X			
Loop Protection		X		
MAC Address Management	X			
MAC Lockdown				X
MAC Lockout				X
MAC-based Authentication				X
Monitoring and Analysis	X			
Network Management Applications (SNMP)	X			
Passwords and Password Clear Protection				X
ProCurve Manager (PCM)	X			
Ping	X			
Port Configuration	X			

Intelligent Edge Software Features	Manual			
	Management and Configuration	Advanced Traffic Management	Multicast and Routing	Access Security Guide
Port Monitoring		X		
Port Security				X
Port Status	X			
Port Trunking (LACP)	X			
Port-Based Access Control (802.1X)				X
Protocol VLANS		X		
Quality of Service (QoS)		X		
RADIUS Authentication and Accounting				X
RADIUS-Based Configuration				X
RMON 1,2,3,9	X			
Secure Copy	X			
SFTP	X			
SNMPv3	X			
Software Downloads (SCP/SFTP, TFPT, Xmodem)	X			
Source-Port Filters				X
Spanning Tree (STP, RSTP, MSTP)		X		
SSHv2 (Secure Shell) Encryption				X
SSL (Secure Socket Layer)				X
Syslog	X			
System Information	X			
TACACS+ Authentication				X
Telnet Access	X			
TFTP	X			
Time Protocols (TimeP, SNTP)	X			
Troubleshooting	X			
Uni-Directional Link Detection (UDLD)	X			

Intelligent Edge Software Features	Manual			
	Management and Configuration	Advanced Traffic Management	Multicast and Routing	Access Security Guide
VLANs		X		
Web Authentication RADIUS Support				X
Web-based Authentication				X
Web UI	X			

1

Getting Started

Contents

Introduction 1-2

Conventions 1-2

- Command Syntax Statements 1-2
- Command Prompts 1-2
- Screen Simulations 1-3
- Configuration and Operation Examples 1-3
- Keys 1-3

Sources for More Information 1-4

- Getting Documentation From the Web 1-6
- Online Help 1-6
  - Menu Interface 1-6
  - Command Line Interface 1-7
  - Web Browser Interface 1-7

Need Only a Quick Start? 1-8

- IP Addressing 1-8

To Set Up and Install the Switch in Your Network 1-8

- Physical Installation 1-8

1

Getting Started

Contents

Introduction 1-2

Conventions 1-2

- Command Syntax Statements 1-2
- Command Prompts 1-2
- Screen Simulations 1-3
- Configuration and Operation Examples 1-3
- Keys 1-3

Sources for More Information 1-4

- Getting Documentation From the Web 1-6
- Online Help 1-6
  - Menu Interface 1-6
  - Command Line Interface 1-7
  - Web Browser Interface 1-7

Need Only a Quick Start? 1-8

- IP Addressing 1-8

To Set Up and Install the Switch in Your Network 1-8

- Physical Installation 1-8

Introduction

This guide is intended for use with the HP ProCurve 6120G/XG and 6120GX switches.

It describes how to use the command line interface (CLI), Menu interface, and web browser to configure, manage, monitor, and troubleshoot switch operation. For an overview of product documentation for the above switches, refer to *"Product Documentation"* on page xiii. You can download documentation from the following web sites:

www.procurve.com/manuals

www.hp.com/go/bladesystem/documentation

h18004.www1.hp.com/products/blades/components/c-class-tech-installing.html

Conventions

This guide uses the following conventions for commands and screen displays.

Command Syntax Statements

Syntax: ip < default-gateway < *ip-addr* >> | routing >

Syntax: show interfaces [*port-list*]

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces (< >) enclose required elements.
- Braces within square brackets ([< >]) indicate a required element within an optional choice.
- Boldface indicates use of a CLI command, part of a CLI command syntax, or other displayed element in general text. For example:

  "Use the **copy tftp** command to download the key from a TFTP server."
- Italics indicate variables for which you must supply a value when executing the command. For example, in this command syntax, you must provide one or more port numbers:

  Syntax: aaa port-access authenticator < *port-list* >

Command Prompts

In the default configuration, your switch displays a CLI prompt similar to the following examples:

```
ProCurve 6120G/XG Blade Switch#

ProCurve 6120XG Blade Switch#
```

To simplify recognition, this guide uses **ProCurve** to represent command prompts. For example:

```
ProCurve#
```

(You can use the **hostname** command to change the text in the CLI prompt.)

Screen Simulations

Displayed Text. Figures containing simulated screen text and command output look like this:

```
ProCurve> show version
Image stamp:    /sw/code/build/vern
                 July 27 2009 13:42:40
                 Z.14.04
                 1037

Boot Image:     Primary

Build Options:  QA

Watchdog:       ENABLED
```

Figure 1-1. Example of a Figure Showing a Simulated Screen

In some cases, brief command-output sequences appear without figure identification. For example:

```
ProCurve(config)# clear public-key
ProCurve(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

Configuration and Operation Examples

Keys

Simulations of actual keys use a bold, sans-serif typeface with square brackets. For example, the Tab key appears as **[Tab]** and the "Y" key appears as **[Y]**.

Sources for More Information

For information about switch operation and features not covered in this guide, consult the following sources:

- Feature Index—For information on which manual to consult for a given software feature, refer to the "Software Feature Index" on page xiv.

Note

For the latest version of all HP ProCurve switch documentation referred to below, including Release Notes covering recently added features, visit any of the following web sites:

www.procurve.com/manuals

www.hp.com/go/bladesystem/documentation

h18004.www1.hp.com/products/blades/components/c-class-tech-installing.html

- Software Release Notes—*Release Notes* provide information on new software updates:
  - new features and how to configure and use them
  - software management, including downloading software to the switch
  - software fixes addressed in current and previous releases
- Product Notes and Software Update Information—The printed *Quick Installation Card* shipped with your switch provides basic installation and getting started information.
- *Installation and Getting Started Guide*—Use the *Installation and Getting Started Guide* to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, as well as describing the LED indications for correct operation and trouble analysis.
- *Management and Configuration Guide*—Use this guide for information on topics such as:
  - various interfaces available on the switch
  - memory and configuration operation
  - interface access
  - IP addressing
  - time protocols
  - port configuration, trunking, and traffic control
  - SNMP, LLDP, and other network management topics

  - file transfers, switch monitoring, troubleshooting, and MAC address management
- *Advanced Traffic Management Guide*—Use this guide for information on topics such as:
  - VLANs: Static port-based and protocol VLANs, and dynamic GVRP VLANs
  - spanning-Tree: 802.1D (STP), 802.1w (RSTP), and 802.1s (MSTP)
  - Quality-of-Service (QoS)
- *Multicast and Routing Guide*—Use this guide for information on topics such as:
  - IGMP
- *Access Security Guide*—Use this guide for information on topics such as:
  - Local username and password security
  - Web-Based and MAC-based authentication
  - RADIUS and TACACS+ authentication
  - SSH (Secure Shell) and SSL (Secure Socket Layer) operation
  - 802.1X access control
  - Port security operation with MAC-based control
  - Authorized IP Manager security
- *IPv6 Configuration Guide*—Use this guide for information on topics such as:
  - Overview of IPv6 operation and features supported
  - Configuring IPv6 addressing
  - Using IPv6 management, security, and troubleshooting features

Getting Documentation From the Web

To obtain the latest versions of documentation and release notes for your switch, go to any of the following web sites:

www.procurve.com/manuals

www.hp.com/go/bladesystem/documentation

h18004.www1.hp.com/products/blades/components/c-class-tech-installing.html

Online Help

Menu Interface

If you need information on specific parameters in the menu interface, refer to the online help provided in the interface. For example:

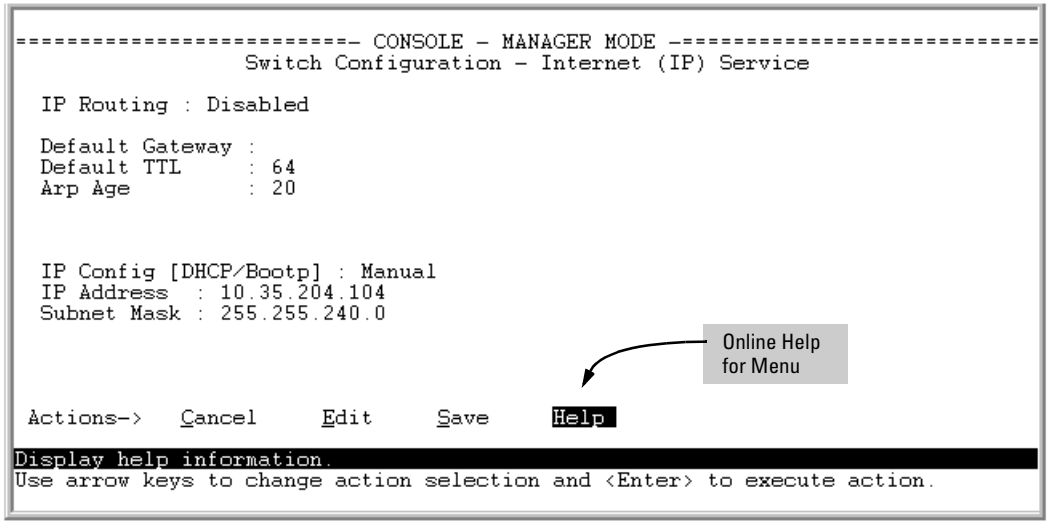

========================= CONSOLE - MANAGER MODE ==========================
Switch Configuration - Internet (IP) Service
IP Routing : Disabled
Default Gateway :
Default TTL : 64
Arp Age : 20
IP Config [DHCP/Bootp] : Manual
IP Address : 10.35.204.104
Subnet Mask : 255.255.240.0
Online Help for Menu
Actions-> Cancel Edit Save Help
Display help information.
Use arrow keys to change action selection and <Enter> to execute action.

Figure 1-2. Online Help for Menu Interface

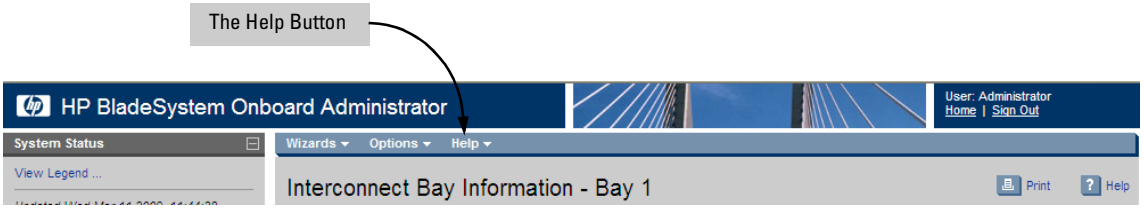


Figure 1-5. Button for Onboard Administrator Interface Online Help

Need Only a Quick Start?

IP Addressing

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, ProCurve recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

- Enter **setup** at the CLI Manager level prompt.

```
Procurve# setup
```

- In the Main Menu of the Menu interface, select

8. Run Setup

For more on using the Switch Setup screen, see the *Installation and Getting Started Guide* you received with the switch.

To Set Up and Install the Switch in Your Network

Physical Installation

Use the *Installation and Getting Started Guide* for the following:

- Notes, cautions, and warnings related to installing and using the switch and its related modules

- Instructions for physically installing the switch in your network
- Quickly assigning an IP address and subnet mask, set a Manager password, and (optionally) configure other basic features.
- Interpreting LED behavior.

For the latest version of the *Installation and Getting Started Guide* for your switch, refer to “Getting Documentation From the Web” on page 1-6.

2

Static Virtual LANs (VLANs)

Contents

Overview 2-3

Introduction 2-4

General VLAN Operation 2-4

Types of Static VLANs Available in the Switch 2-5

Port-Based VLANs 2-5

Protocol-Based VLANs 2-5

Designated VLANs 2-5

Terminology 2-6

Static VLAN Operation 2-7

VLAN Environments 2-8

VLAN Operation 2-9

Overlapping (Tagged) VLANs 2-10

Per-Port Static VLAN Configuration Options 2-12

VLAN Operating Rules 2-13

General Steps for Using VLANs 2-16

Multiple VLAN Considerations 2-17

Single Forwarding Database Operation 2-17

Example of an Unsupported Configuration and How To Correct It 2-19

Multiple Forwarding Database Operation 2-20

Configuring VLANs 2-21

Menu: Configuring Port-Based VLAN Parameters 2-21

To Change VLAN Support Settings 2-22

Adding or Editing VLAN Names 2-23

Adding or Changing a VLAN Port Assignment 2-25

CLI: Configuring Port-Based and Protocol-Based VLAN Parameters 2-27

Web: Viewing and Configuring VLAN Parameters 2-39

802.1Q VLAN Tagging 2-40

Special VLAN Types 2-45

VLAN Support and the Default VLAN 2-45

The Primary VLAN 2-45

The Secure Management VLAN 2-46

Preparation 2-48

Configuration 2-49

. 2-49

Using DHCP to Obtain an IP Address 2-50

Deleting the Management VLAN 2-53

Operating Notes for Management VLANs 2-53

Voice VLANs 2-54

Operating Rules for Voice VLANs 2-54

Components of Voice VLAN Operation 2-55

Voice VLAN Access Security 2-55

Effect of VLANs on Other Switch Features 2-55

Spanning Tree Operation with VLANs 2-55

IP Interfaces 2-56

VLAN MAC Address 2-56

Port Trunks 2-56

Port Monitoring 2-56

Jumbo Packet Support 2-57

VLAN Restrictions 2-57

Overview

This chapter describes how to configure and use static, port-based and protocol-based VLANs on the switches covered in this guide.

For general information on how to use the switch's built-in interfaces, refer to these chapters in the *Management and Configuration Guide* for your switch:

- Chapter 3, "Using the Menu Interface"
- Chapter 4, "Using the Command Line Interface (CLI)"
- Chapter 5, "Using the Web Browser Interface
- Chapter 6, "Switch Memory and Configuration"

Introduction

VLAN Features

Feature	Default	Menu	CLI	Web
view existing VLANs	n/a	page 2-22 thru 2-27	page 2-28	page 2-39
configuring static VLANs	default VLAN with VID = 1	page 2-22 thru 2-27	page 2-27	page 2-39

VLANs enable you to group users by logical function instead of physical location. This helps to control bandwidth usage within your network by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources and/or their use of individual protocols. You can also improve traffic control at the edge of your network by separating traffic of different protocol types. VLANs can also enhance your network security by creating separate subnets to help control in-band access to specific network resources.

General VLAN Operation

A VLAN is comprised of multiple ports operating as members of the same subnet (broadcast domain). Ports on multiple devices can belong to the same VLAN, and traffic moving between ports in the same VLAN is bridged (or "switched"). (Traffic moving between different VLANs must be routed.) A s*tatic* VLAN is an 802.1Q-compliant VLAN configured with one or more ports that remain members regardless of traffic usage. (A *dynamic* VLAN is an 802.1Q-compliant VLAN membership that the switch temporarily creates on a port to provide a link to another port in the same VLAN on another device.)

This chapter describes *static* VLANs configured for port-based or protocol-based operation. Static VLANs are configured with a name, VLAN ID number (VID), and port members. (For *dynamic* VLANs, refer to chapter 3, "GVRP" .)

By default, the switches covered in this guide are 802.1Q VLAN-enabled and allow up to 256 static and dynamic VLANs. (The default static VLAN setting is 8). 802.1Q compatibility enables you to assign each switch port to multiple VLANs, if needed.

Types of Static VLANs Available in the Switch

Port-Based VLANs

This type of static VLAN creates a specific layer-2 broadcast domain comprised of member ports that bridge IPv4 traffic among themselves. Port-Based VLAN traffic is routable on the switches covered in this guide.

Protocol-Based VLANs

This type of static VLAN creates a layer-3 broadcast domain for traffic of a particular protocol, and is comprised of member ports that bridge traffic of the specified protocol type among themselves. Some protocol types are routable on the switches covered in this guide. Refer to table 2-1 on page 2-7.

Designated VLANs

The switch uses these static, port-based VLAN types to separate switch management traffic from other network traffic. While these VLANs are not limited to management traffic only, they can provide improved security and availability for management traffic.

- **The Default VLAN:** This port-based VLAN is always present in the switch and, in the default configuration, includes all ports as members (page 2-45).
- **The Primary VLAN:** The switch uses this port-based VLAN to run certain features and management functions, including DHCP/Bootp responses for switch management. In the default configuration, the Default VLAN is also the Primary VLAN. However, you can designate another, port-based, non-default VLAN, as the Primary VLAN (page 2-45).
- **The Secure Management VLAN:** This optional, port-based VLAN establishes an isolated network for managing the ProCurve switches that support this feature. Access to this VLAN and to the switch's management functions are available only through ports configured as members (page 2-46).
- **Voice VLANs:** This optional, port-based VLAN type enables you to separate, prioritize, and authenticate voice traffic moving through your network, and to avoid the possibility of broadcast storms affecting VoIP (Voice-over-IP) operation (page 2-54).

Note

In a multiple-VLAN environment that includes some older switch models there may be problems related to the same MAC address appearing on different ports and VLANs on the same switch. In such cases the solution is to impose some cabling and VLAN restrictions. For more on this topic, refer to "Multiple VLAN Considerations" on page 2-17.

Terminology

Dynamic VLAN: An 802.1Q VLAN membership temporarily created on a port linked to another device, where both devices are running GVRP. (See also **Static VLAN**.) For more information, refer to chapter 3, "GVRP" .

Static VLAN: A port-based or protocol-based VLAN configured in switch memory. (See also **Dynamic VLAN**.)

Tagged Packet: A packet that carries an IEEE 802.1Q VLAN ID (VID), which is a two-byte extension that precedes the source MAC address field of an ethernet frame. A VLAN tag is layer 2 data and is transparent to higher layers.

Tagged VLAN: A VLAN that complies with the 802.1Q standard, including priority settings, and allows a port to join multiple VLANs. (See also **Untagged VLAN**.)

Untagged Packet: A packet that does not carry an IEEE 802.1Q VLAN ID (VID).

Untagged VLAN: A VLAN that does not use or forward 802.1Q VLAN tagging, including priority settings. A port can be a member of only one untagged VLAN of a given type (port-based and the various protocol-based types). (See also **Tagged VLAN**.)

VID: The acronym for a VLAN Identification Number. Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN must be given the same VID in every device in which it is configured.

Static VLAN Operation

A group of networked ports assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on the switch. On a given switch, packets are bridged between source and destination ports that belong to the same VLAN. Thus, all ports passing traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out all ports.

Table 2-1. Comparative Operation of Port-Based and Protocol-Based VLANs

	Port-Based VLANs	Protocol-Based VLANs
IP Addressing	Usually configured with at least one unique IP address. You can create a port-based VLAN without an IP address. However, this limits the switch features available to ports on that VLAN. (Refer to "How IP Addressing Affects Switch Operation" in the chapter "Configuring IP Addressing" in the *Management and Configuration Guide* for the switch.) You can also use multiple IP addresses to create multiple subnets within the same VLAN. (For more on this topic, refer to the chapter on "Configuring IP Addressing" in the *Management and Configuration Guide* for the switch.)	You can configure IP addresses on all protocol VLANs. However, IP addressing is used only on IPv4 and IPv6 protocol VLANs. The maximum number of IP addresses supported on a switch is 256. Each IP address that you configure on a VLAN interface must be unique in the switch. For more information, refer to the chapter on "Configuring IP Addressing" in the *Management and Configuration Guide*.
Untagged VLAN Membership	A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	A port can be an untagged member of one protocol VLAN of a specific protocol type (such as IPX or IPv6). If the same protocol type is configured in multiple protocol VLANs, then a port can be an untagged member of only one of those protocol VLANs. For example, if you have two protocol VLANs, 100 and 200, and both include IPX, then a port can be an untagged member of either VLAN 100 or VLAN 200, but not both VLANs. A port's untagged VLAN memberships can include up to four different protocol types. This means that a port can be an untagged member of one of the following: • Four single-protocol VLANs • Two protocol VLANs where one VLAN includes a single protocol and the other includes up to three protocols • One protocol VLAN where the VLAN includes four protocols

	Port-Based VLANs	Protocol-Based VLANs
Tagged VLAN Membership	A port can be a tagged member of any port-based VLAN. See above.	A port can be a tagged member of any protocol-based VLAN. See above.
Commands for Configuring Static VLANs	vlan < ***VID*** > [tagged | untagged < [e] ***port-list*** >]	vlan < *VID* > protocol < ipx | ipv4 | ipv6 | arp | appletalk | sna | netbeui > vlan < *VID* > [tagged | untagged < [e] ***port-list*** >]

VLAN Environments

You can configure different VLAN types in any combination. Note that the default VLAN will always be present. (For more on the default VLAN, refer to "VLAN Support and the Default VLAN" on page 2-45.)

Table 2-2. VLAN Environments

VLAN Environment	Elements
The default VLAN (port-based; VID of "1") Only	In the default VLAN configuration, all ports belong to VLAN 1 as untagged members. VLAN 1 is a port-based VLAN, for IPv4 traffic.
Multiple VLAN Environment	In addition to the default VLAN, the configuration can include one or more other port-based VLANs and one or more protocol VLANs. (The switches covered in this guide allow up to 256 (vids up to 4094) VLANs of all types.) Using VLAN tagging, ports can belong to multiple VLANs of all types. Enabling routing on the switch enables the switch to route IPv4 traffic between port-based VLANs and between port-based VLANs and IPv4 protocol VLANs. Routing other types of traffic between VLANs requires an external router capable of processing the appropriate protocol(s).

VLAN Operation

The Default VLAN. In figure 2-1, all ports belong to the default VLAN, and devices connected to these ports are in the same broadcast domain. Except for an IP address and subnet, no configuration steps are needed.

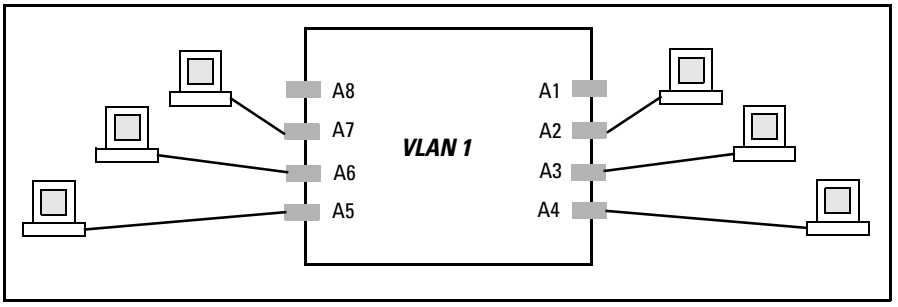


Figure 2-1. Example of a Switch in the Default VLAN Configuration

Multiple Port-Based VLANs. In figure 2-2, routing within the switch is disabled (the default). This means that communication between any routable VLANs on the switch must go through the external router. In this case, VLANs "W" and "X" can exchange traffic through the external router, but traffic in VLANs "Y" and "Z" is restricted to the respective VLANs. Note that VLAN 1, the default VLAN, is also present, but not shown. (The default VLAN cannot be deleted from the switch. However, ports assigned to other VLANs can be removed from the default VLAN, if desired.) If internal (IP) routing is enabled on the switch, then the external router is not needed for traffic to move between port-based VLANs.

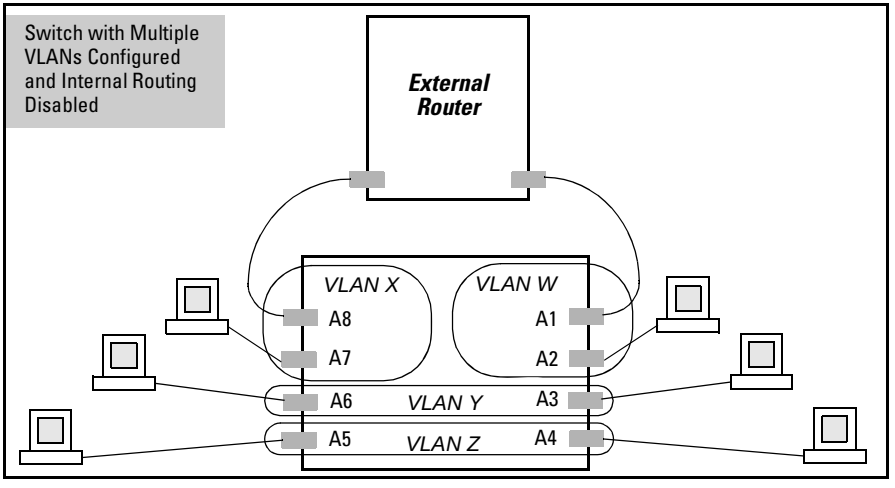


Figure 2-2. Example of Multiple VLANs on the Switch

Protocol VLAN Environment. Figure 2-2 can also be applied to a protocol VLAN environment. In this case, VLANs "W" and "X" represent routable protocol VLANs. VLANs "Y" and "Z" can be any protocol VLAN. As noted for the discussion of multiple port-based VLANs, VLAN 1 is not shown. Enabling internal (IP) routing on the switch allows IP traffic to move between VLANs on the switch. However, routable, non-IP traffic always requires an external router.

Overlapping (Tagged) VLANs

A port can be a member of more than one VLAN of the same type if the device to which the port connects complies with the 802.1Q VLAN standard. For example, a port connected to a central server using a network interface card (NIC) that complies with the 802.1Q standard can be a member of multiple VLANs, allowing members of multiple VLANs to use the server. Although these VLANs cannot communicate with each other through the server, they can all access the server over the same connection from the switch. Where VLANs overlap in this way, VLAN "tags" are used in the individual packets to distinguish between traffic from different VLANs. A VLAN tag includes the particular VLAN I.D. (VID) of the VLAN on which the packet was generated.

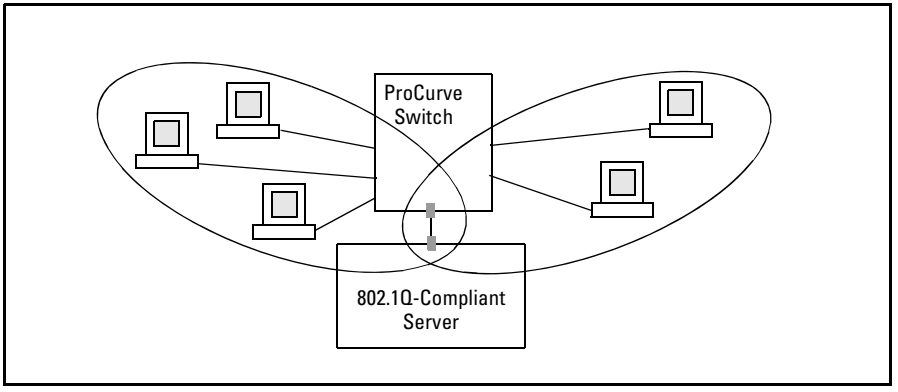


Figure 2-3. Example of Overlapping VLANs Using the Same Server

Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through a single switch-to-switch link.

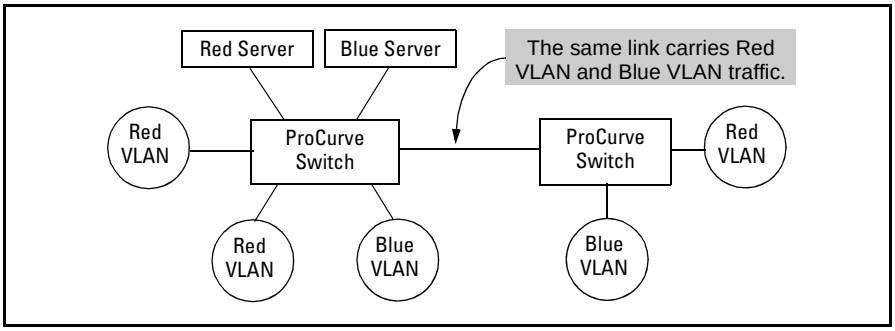


Figure 2-4. Example of Connecting Multiple VLANs Through the Same Link

Introducing Tagged VLAN Technology into Networks Running Legacy (Untagged) VLANs. You can introduce 802.1Q-compliant devices into networks that have built untagged VLANs based on earlier VLAN technology. The fundamental rule is that legacy/untagged VLANs require a separate link for each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one link. This means that on the 802.1Q-compliant device, separate ports (configured as untagged) must be used to connect separate VLANs to non-802.1Q devices.

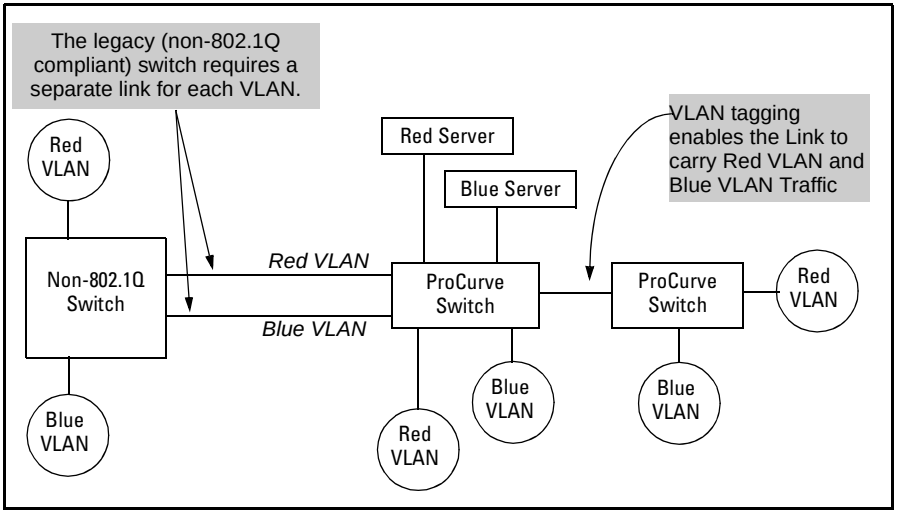


Figure 2-5. Example of Tagged and Untagged VLAN Technology in the Same Network

For more information on VLANs, refer to:

- "Overview of Using VLANs" (page 2-45)
- "Menu: Configuring VLAN Parameters (page 2-21)

- "CLI: Configuring VLAN Parameters" (page 2-21)
- "Web: Viewing and Configuring VLAN Parameters" (page 2-39)
- "VLAN Tagging Information" (page 2-40)
- "Effect of VLANs on Other Switch Features" (page 2-55)
- "VLAN Restrictions" (page 2-57)

Per-Port Static VLAN Configuration Options

The following figure and table show the options you can use to assign individual ports to a static VLAN. Note that GVRP, if configured, affects these options and VLAN behavior on the switch. The display below shows the per-port VLAN configuration options. Table 2-3 briefly describes these options.

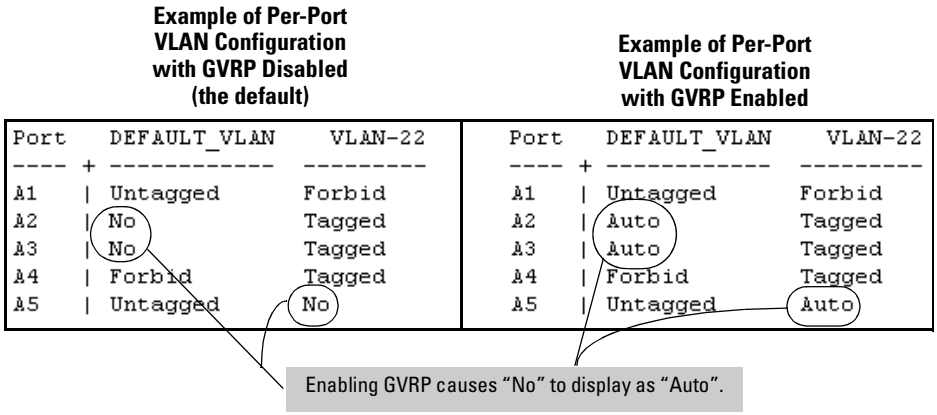

Example of Per-Port VLAN Configuration with GVRP Disabled (the default)
Example of Per-Port VLAN Configuration with GVRP Enabled
Port DEFAULT_VLAN VLAN-22
A1 Untagged Forbid
A2 No Tagged
A3 No Tagged
A4 Forbid Tagged
A5 Untagged No
Port DEFAULT_VLAN VLAN-22
A1 Untagged Forbid
A2 Auto Tagged
A3 Auto Tagged
A4 Forbid Tagged
A5 Untagged Auto
Enabling GVRP causes "No" to display as "Auto".

Figure 2-6. Comparing Per-Port VLAN Options With and Without GVRP

Table 2-3. Per-Port VLAN Configuration Options

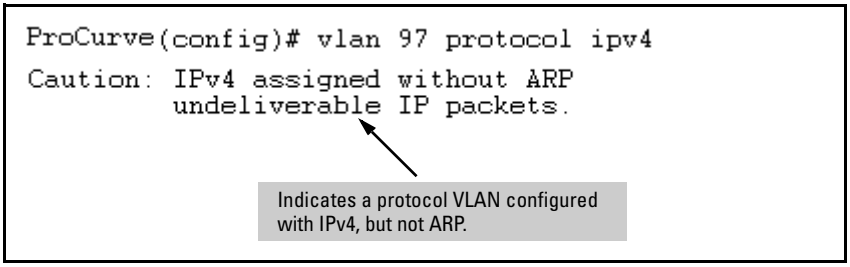
Parameter	Effect on Port Participation in Designated VLAN
Tagged	Allows the port to join multiple VLANs.
Untagged	Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN. A port can be an untagged member of only one port-based VLAN. A port can also be an untagged member of only one protocol-based VLAN for any given protocol type. For example, if the switch is configured with the default VLAN plus three protocol-based VLANs that include IPX, then port 1 can be an untagged member of the default VLAN and one of the protocol-based VLANS.

Parameter	Effect on Port Participation in Designated VLAN
No **- or -** **Auto**	**No**: Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN. **Auto**: Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID
Forbid	Prevents the port from joining the VLAN, even if GVRP is enabled on the switch.

VLAN Operating Rules

- **DHCP/Bootp:** If you are using DHCP/Bootp to acquire the switch's configuration, packet time-to-live, and TimeP information, you must designate the VLAN on which DHCP is configured for this purpose as the Primary VLAN. (In the factory-default configuration, the DEFAULT_VLAN is the Primary VLAN.)
- **Per-VLAN Features:** IGMP and some other features operate on a "per VLAN" basis. This means you must configure such features separately for each VLAN in which you want them to operate.
- **Default VLAN:** You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.
- **VLAN Port Assignments:** Any ports *not* specifically removed from the default VLAN remain in the DEFAULT_VLAN, regardless of other port assignments. Also, a port must always be a tagged or untagged member of at least one port-based VLAN.
- **Voice-Over-IP (VoIP):** VoIP operates only over static, port-based VLANs.
- **Multiple VLAN Types Configured on the Same Port:** A port can simultaneously belong to both port-based and protocol-based VLANs.
- **Protocol Capacity:** A protocol-based VLAN can include up to four protocol types. In protocol VLANs using the IPv4 protocol, ARP must be one of these protocol types (to support normal IP network operation). Otherwise, IP traffic on the VLAN is disabled. If you configure an IPv4

protocol VLAN that does not already include the ARP VLAN protocol, the switch displays this message:


ProCurve(config)# vlan 97 protocol ipv4
Caution: IPv4 assigned without ARP
undeliverable IP packets.
Indicates a protocol VLAN configured with IPv4, but not ARP.

- **Deleting Static VLANs:** On the switches covered in this guide you can delete a VLAN regardless of whether there are currently any ports belonging to that VLAN. (The ports are moved to the default VLAN.)
- **Adding or Deleting VLANs:** Changing the number of VLANs supported on the switch requires a reboot. (From the CLI, you must perform a **write memory** command before rebooting.) Other VLAN configuration changes are dynamic.
- **Inbound Tagged Packets:** If a tagged packet arrives on a port that is not a tagged member of the VLAN indicated by the packet's VID, the switch drops the packet. Similarly, the switch will drop an inbound, tagged packet if the receiving port is an *untagged* member of the VLAN indicated by the packet's VID.
- **Untagged Packet Forwarding:** To enable an inbound port to forward an untagged packet, the port must be an untagged member of either a protocol VLAN matching the packet's protocol or an untagged member of a port-based VLAN. That is, when a port receives an incoming, untagged packet, it processes the packet according to the following ordered criteria:
  a. If the port has no untagged VLAN memberships, the switch drops the packet.
  b. If the port has an untagged VLAN membership in a protocol VLAN that matches the protocol type of the incoming packet, then the switch forwards the packet on that VLAN.
  c. If the port is a member of an untagged, port-based VLAN, the switch forwards the packet to that VLAN. Otherwise, the switch drops the packet.

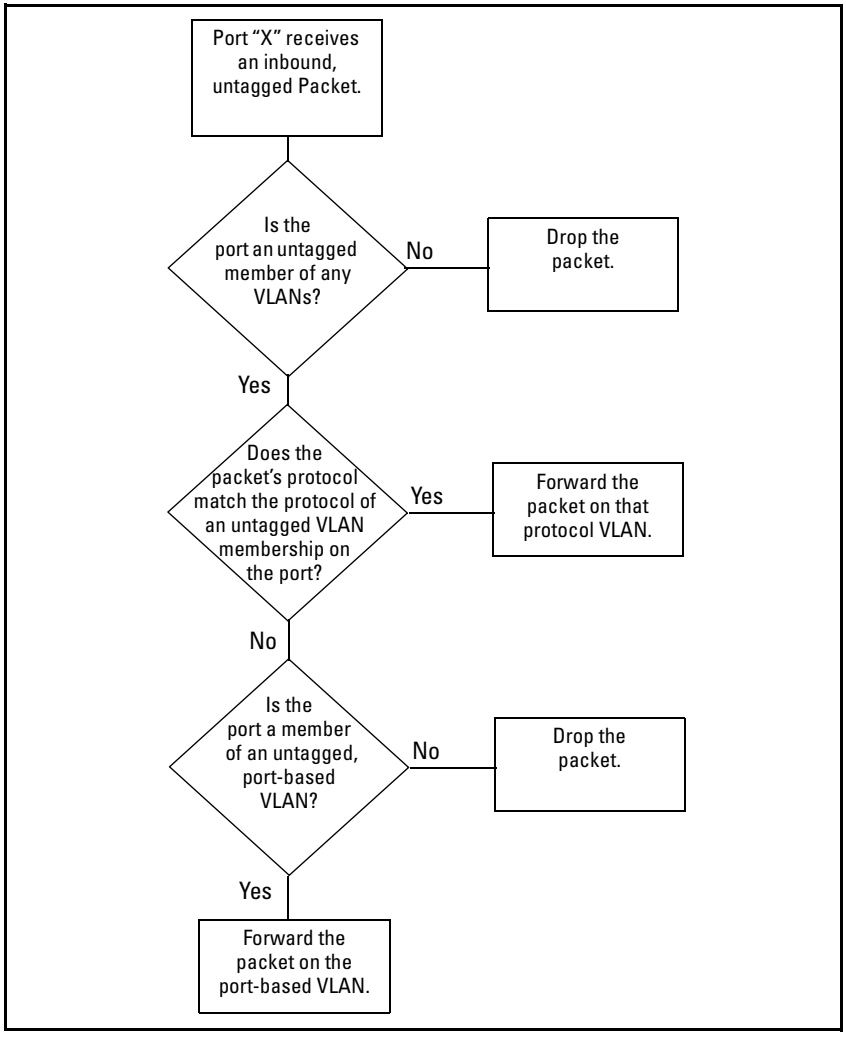

Port "X" receives an inbound, untagged Packet.
Is the port an untagged member of any VLANs?
No
Drop the packet.
Yes
Does the packet's protocol match the protocol of an untagged VLAN membership on the port?
Yes
Forward the packet on that protocol VLAN.
No
Is the port a member of an untagged, port-based VLAN?
No
Drop the packet.
Yes
Forward the packet on the port-based VLAN.

Figure 2-7. Untagged VLAN Operation

- **Tagged Packet Forwarding:** If a port is a tagged member of the same VLAN as an inbound, tagged packet received on that port, then the switch forwards the packet to an outbound port on that VLAN. (To enable the forwarding of tagged packets, any VLAN to which the port belongs as a

tagged member must have the same VID as that carried by the inbound, tagged packets generated on that VLAN.)

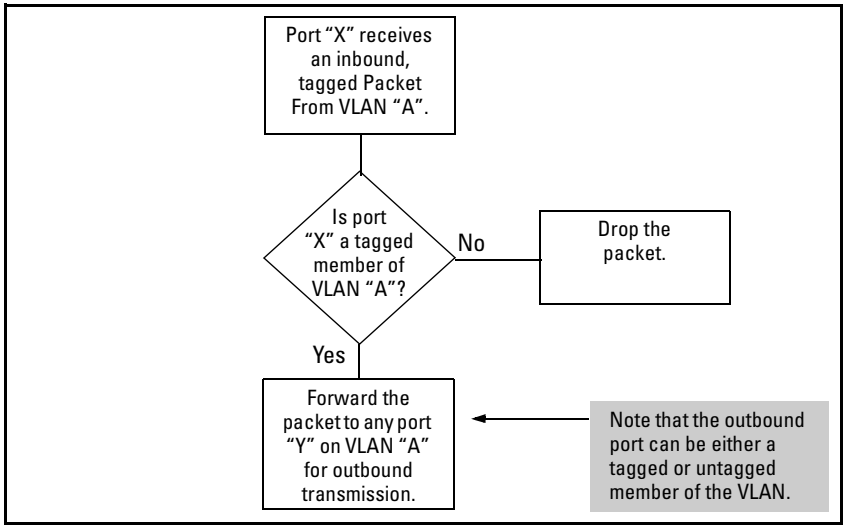

Port "X" receives an inbound, tagged Packet From VLAN "A".
Is port "X" a tagged member of VLAN "A"?
No
Drop the packet.
Yes
Forward the packet to any port "Y" on VLAN "A" for outbound transmission.
Note that the outbound port can be either a tagged or untagged member of the VLAN.

Figure 2-8. Tagged VLAN Operation

See also "Multiple VLAN Considerations" on page 2-17.

General Steps for Using VLANs

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, port trunking, and IGMP. (Refer to "Effect of VLANs on Other Switch Features" on page 2-55.) If you plan on using dynamic VLANs, include the port configuration planning necessary to support this feature. (Refer to chapter 3, "GVRP" .)

   By default, VLAN support is enabled for up to 256 VLANs.

2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired switch ports to the new VLAN(s).
4. If you are managing VLANs with SNMP in an IP network, the VLAN through which you are managing the switch must have an IP address. For information on the procedure and restrictions when you configure an IP address on a VLAN interface, refer to Table 2-1 on page 2-7.

Multiple VLAN Considerations

Switches use a *forwarding database* to maintain awareness of which external devices are located on which VLANs. Some switches, such as the switches covered in this guide, have a *multiple forwarding database*, which means the switch allows multiple database entries of the same MAC address, with each entry showing the (different) source VLAN and source port. Other switch models have a *single forwarding database*, which means they allow only one database entry of a unique MAC address, along with the source VLAN and source port on which it is found. All VLANs on a switch use the same MAC address. Thus, connecting a multiple forwarding database switch to a single forwarding database switch where multiple VLANs exist imposes some cabling and port VLAN assignment restrictions. Table 2-4 illustrates the functional difference between the two database types.

Table 2-4. Example of Forwarding Database Content

Multiple Forwarding Database		
MAC Address	**Destination VLAN ID**	**Destination Port**
0004ea-84d9f4	1	A5
0004ea-84d9f4	22	A12
0004ea-84d9f4	44	A20
0060b0-880a81	33	A20
This database allows multiple destinations for the same MAC address. If the switch detects a new destination for an existing MAC entry, it just **adds** a new instance of that MAC to the table.		

Single Forwarding Database		
MAC Address	**Destination VLAN ID**	**Destination Port**
0004ea-84d9f4	100	A9
0060b0-880af9	105	A10
0060b0-880a81	107	A17
This database allows only one destination for a MAC address. If the switch detects a new destination for an existing MAC entry, it **replaces** the existing MAC instance with a new instance showing the new destination.		

To determine whether other vendors' devices use single-forwarding or multiple-forwarding database architectures, refer to the documentation provided for those devices.

Single Forwarding Database Operation

When a packet arrives with a destination MAC address that matches a MAC address in the switch's forwarding table, the switch tries to send the packet to the port listed for that MAC address. But, if the destination port is in a different VLAN than the VLAN on which the packet was received, the switch

drops the packet. This is not a problem for a switch with a multiple forwarding database because the switch allows multiple instances of a given MAC address; one for each valid destination. However, a switch with a single forwarding database allows only one instance of a given MAC address. If (1) you connect the two types of switches through multiple ports or trunks belonging to different VLANs, and (2) enable routing on the switch having the multiple forwarding database; then, on the switch having the single forwarding database, the port and VLAN record it maintains for the connected multiple-forwarding-database switch can frequently change. This causes poor performance and the appearance of an intermittent or broken connection.

Example of an Unsupported Configuration and How To Correct It

The Problem. In figure 2-9, the MAC address table for Switch 6600 will sometimes record the switch as accessed on port A1 (VLAN 1), and other times as accessed on port B1 (VLAN 2):

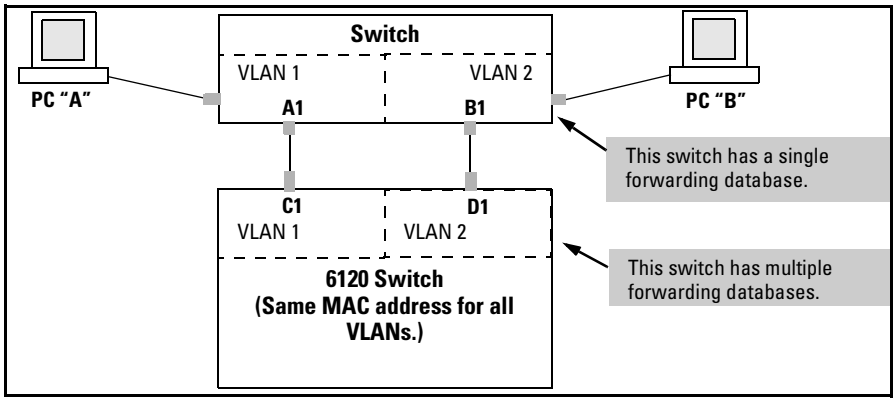


Figure 2-9. Example of Invalid Configuration for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

In figure 2-9, PC "A" sends an IP packet to PC "B".

1. The packet enters VLAN 1 in the Switch 6600 with the 6120 switch's MAC address in the destination field. Because the 6600 has not yet learned this MAC address, it does not find the address in its address table, and floods the packet out all ports, including the VLAN 1 link (port "A1") to the 6120 switch. The 6120 switch then routes the packet through the VLAN 2 link to the 6600, which forwards the packet on to PC "B". Because the 6600 received the packet from the 6120 switch on VLAN 2 (port "B1"), the 6600's single forwarding database records the 6120 switch as being on port "B1" (VLAN 2).
2. PC "A" now sends a second packet to PC "B". The packet again enters VLAN 1 in the Switch 6600 with the 6120 switch's MAC address in the destination field. However, this time the Switch 6600's single forwarding database indicates that the 6120 is on port B1 (VLAN 2), and the 6600 drops the packet instead of forwarding it.
3. Later, the 6120 switch transmits a packet to the 6600 through the VLAN 1 link, and the 6600 updates its address table to indicate that the 6120 switch is on port A1 (VLAN 1) instead of port B1 (VLAN 2). Thus, the 6600's information on the location of the 6120 switch changes over time. For this

reason, the 6600 discards some packets directed through it for the 6120 switch, resulting in poor performance and the appearance of an intermittent or broken link.

The Solution. To avoid the preceding problem, use only one cable or port trunk between the single-forwarding and multiple-forwarding database devices, and configure the link with multiple, tagged VLANs.

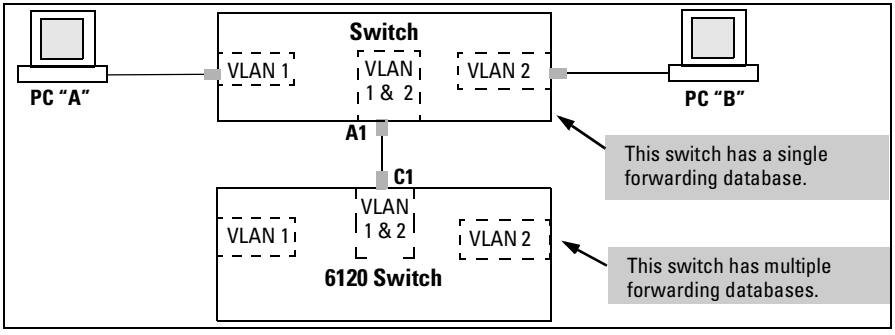


Figure 2-10. Example of a Solution for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

Now, the 6600 forwarding database always lists the 6120 MAC address on port A1, and the 6600 will send traffic to either VLAN on the 6120.

To increase the network bandwidth of the connection between the devices, you can use a trunk of multiple physical links rather than a single physical link.

Multiple Forwarding Database Operation

If you want to connect one of the switches covered by this guide to another switch that has a multiple forwarding database, you can use either or both of the following connection options:

- A separate port or port trunk interface for each VLAN. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs and port numbers. (See table 2-4.) The fact that the switches covered by this guide use the same MAC address on all VLAN interfaces causes no problems.
- The same port or port trunk interface for multiple (tagged) VLANs. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs, but the same port number.

Allowing multiple entries of the same MAC address on different VLANs enables topologies such as the following:

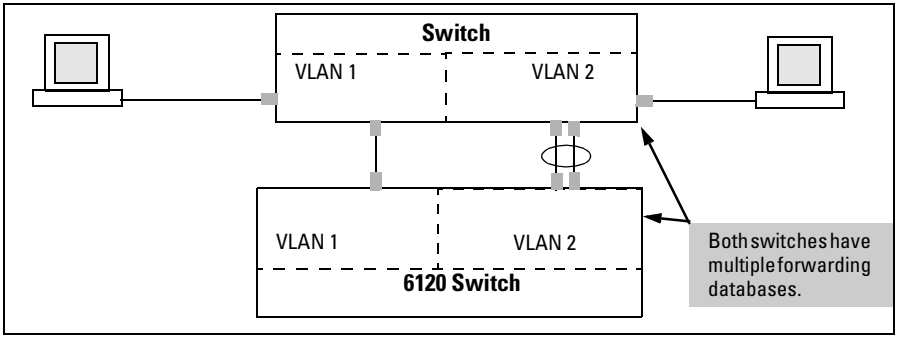


Figure 2-11. Example of a Valid Topology for Devices Having Multiple Forwarding Databases in a Multiple VLAN Environment

Configuring VLANs

Menu: Configuring Port-Based VLAN Parameters

The Menu interface enables you to configure and view port-based VLANs.

Note

The Menu interface configures and displays only port-based VLANs. The CLI configures and displays port-based *and* protocol-based VLANs (page 2-27).

In the factory default state, support is enabled for up to 256 VLANs. (You can reconfigure the switch to support up to 256 (vids up to 4094) VLANs.) Also, in the default configuration, all ports on the switch belong to the default VLAN and are in the same broadcast/multicast domain. (The default VLAN is also the default Primary VLAN—refer to "The Primary VLAN" on page 2-45.) In addition to the default VLAN, you can configure additional static VLANs by adding new VLAN names and VIDs, and then assigning one or more ports to each VLAN. (The maximum of 256 VLANs includes the default VLAN, all additional static VLANs you configure, and any dynamic VLANs the switch creates if you enable GVRP—page 3-1.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See "802.1Q VLAN Tagging" on page 2-40.)

To Change VLAN Support Settings

This section describes:

- Changing the maximum number of VLANs to support
- Changing the Primary VLAN selection (See "Changing the Primary VLAN" on page 2-34.)
- Enabling or disabling dynamic VLANs (Refer to chapter 3, "GVRP" .)

1. From the Main Menu select:

   2. Switch Configuration

   8. VLAN Menu ...

   1. VLAN Support

   You will then see the following screen:

```
============================ CONSOLE - MANAGER MODE ============================
                    Switch Configuration - VLAN - VLAN Support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : No

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure 2-12. The Default VLAN Support Screen

2. Press **[E]** (for **Edit**), then do one or more of the following:
   - To change the maximum number of VLANs, type the new number (1 - 256 allowed; default 256).
   - To designate a different VLAN as the Primary VLAN, select the **Primary VLAN** field and use the space bar to select from the existing options. (Note that the Primary VLAN must be a static, port-based VLAN.)
   - To enable or disable dynamic VLANs, select the **GVRP Enabled** field and use the Space bar to toggle between options. (For GVRP information, refer to chapter 3, "GVRP" .)

Note

For optimal switch memory utilization, set the number of VLANs at the number you will likely be using or a few more. If you need more VLANs later, you can increase this number, but a switch reboot will be required at that time.

3. Press **[Enter]** and then **[S]** to save the VLAN support configuration and return to the VLAN Menu screen.

If you changed the value for **Maximum VLANs to support**, you will see an asterisk next to the **VLAN Support** option (see below).

An asterisk indicates you must reboot the switch to implement the new Maximum VLANs setting.

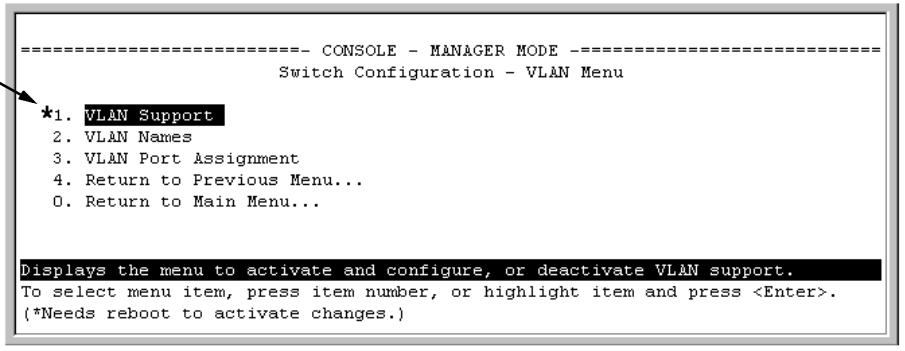

========== CONSOLE - MANAGER MODE ==========
Switch Configuration - VLAN Menu
*1. VLAN Support
2. VLAN Names
3. VLAN Port Assignment
4. Return to Previous Menu...
0. Return to Main Menu...
Displays the menu to activate and configure, or deactivate VLAN support.
To select menu item, press item number, or highlight item and press <Enter>.
(*Needs reboot to activate changes.)

Figure 2-13. VLAN Menu Screen Indicating the Need To Reboot the Switch

- If you changed the VLAN Support option, you must reboot the switch before the Maximum VLANs change can take effect. You can go on to configure other VLAN parameters first, but remember to reboot the switch when you are finished.
- If you did not change the VLAN Support option, a reboot is not necessary.

4. Press **[0]** to return to the Main Menu.

Adding or Editing VLAN Names

Use this procedure to add a new VLAN or to edit the name of an existing VLAN.

1. From the Main Menu select:

   2. Switch Configuration
   8. VLAN Menu …
   2. VLAN Names

   If multiple VLANs are not yet configured you will see a screen similar to figure 2-14:

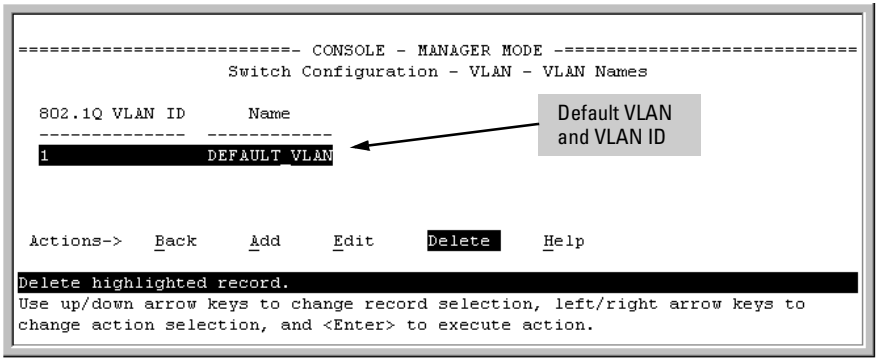

========== CONSOLE - MANAGER MODE ==========
Switch Configuration - VLAN - VLAN Names
802.1Q VLAN ID
Name
1
DEFAULT_VLAN
Default VLAN and VLAN ID
Actions-> Back Add Edit Delete Help
Delete highlighted record.
Use up/down arrow keys to change record selection, left/right arrow keys to change action selection, and <Enter> to execute action.

Figure 2-14. The Default VLAN Names Screen

2. Press **[A]** (for **Add**). You will then be prompted for a new VLAN name and VLAN ID:

   802.1Q VLAN ID : 1
   Name : _

3. Type in a VID (VLAN ID number). This can be any number from 2 to 4094 that is not already being used by another VLAN. (The switch reserves "1" for the default VLAN.)

   Remember that a VLAN *must* have the same VID in every switch in which you configure that same VLAN. (GVRP dynamically extends VLANs with correct VID numbering to other switches. Refer to chapter 3, "GVRP" .)

4. Press ↓ to move the cursor to the **Name** line and type the VLAN name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press **[Enter]**.
   (Avoid these characters in VLAN names: **@, #, $, ^, &, ***, **(**, and **)**.)

5. Press **[S]** (for **Save**). You will then see the VLAN Names screen with the new VLAN listed.

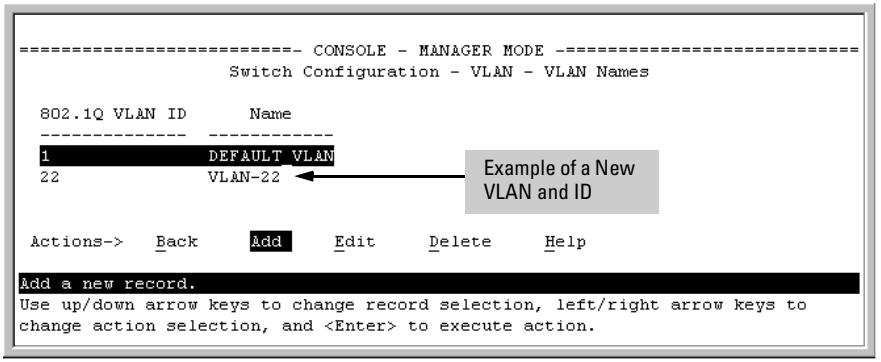

========== CONSOLE - MANAGER MODE ==========
Switch Configuration - VLAN - VLAN Names
802.1Q VLAN ID
Name
1
DEFAULT_VLAN
22
VLAN-22
Example of a New VLAN and ID
Actions-> Back Add Edit Delete Help
Add a new record.
Use up/down arrow keys to change record selection, left/right arrow keys to change action selection, and <Enter> to execute action.

Figure 2-15. Example of VLAN Names Screen with a New VLAN Added

6. Repeat steps 2 through 5 to add more VLANs.

   Remember that you can add VLANs until you reach the number specified in the **Maximum VLANs to support** field on the VLAN Support screen (see figure 2-12 on page 2-22). This includes any VLANs added dynamically due to GVRP operation.

7. Return to the VLAN Menu to assign ports to the new VLAN(s) as described in the next section, "Adding or Changing a VLAN Port Assignment".

Adding or Changing a VLAN Port Assignment

Use this procedure to add ports to a VLAN or to change the VLAN assignment(s) for any port. (Ports not specifically assigned to a VLAN are automatically in the default VLAN.)

1. From the Main Menu select:

   2. Switch Configuration

   8. VLAN Menu ...

   3. VLAN Port Assignment

   You will then see a VLAN Port Assignment screen similar to the following:

Note

The "VLAN Port Assignment" screen displays up to 32 static, port-based VLANs in ascending order, by VID. If the switch configuration includes more than 32 such VLANs, use the CLI **show vlans [VID | ports < *port-list* >]** command to list data on VLANs having VIDs numbered sequentially higher than the first 32.

Default: In this example, the "VLAN-22" has been defined, but no ports have yet been assigned to it. ("No" means the port is not assigned to that VLAN.)
Using GVRP? If you plan on using GVRP, any ports you don't want to join should be changed to "Forbid".

A port can be assigned to several VLANs, but only one of those assignments can be "Untagged".

```
==========================- CONSOLE - MANAGER MODE -=============================
                Switch Configuration - VLAN - VLAN Port Assignment

  Port   DEFAULT_VLAN    VLAN-22       |  Port   DEFAULT_VLAN    VLAN-22
  ---- + ------------  ------------    |  ---- + ------------  ------------
 A1    | Untagged      No              |  A8   | Untagged      No
 A2    | Tagged        No              |  A9   | Untagged      No
 A3    | Untagged      No              |  A10  | Untagged      No
 A4    | Untagged      No              |  A11  | Untagged      No
 A5    | Untagged      No              |  A12  | Untagged      No
 A6    | Untagged      No              |  A13  | Untagged      No
 A7    | Untagged      No              |  A14  | Untagged      No

 Actions->   Cancel    Edit    Save    Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure 2-16. Example of the Port-Based VLAN Port Assignment Screen in the Menu Interface

2. To change a port's VLAN assignment(s):
   a. Press **[E]** (for **Edit**).
   b. Use the arrow keys to select a VLAN assignment you want to change.
   c. Press the Space bar to make your assignment selection (**No**, **Tagged**, **Untagged**, or **Forbid**).

Note

For GVRP Operation: If you enable GVRP on the switch, "**No**" converts to "**Auto**", which allows the VLAN to dynamically join an advertised VLAN that has the same VID. See "Per-Port Options for Dynamic VLAN Advertising and Joining" on page 3-9.

Untagged VLANs: Only one untagged VLAN is allowed per port. Also, there must be at least one VLAN assigned to each port. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN).

For example, if you want ports A4 and A5 to belong to both DEFAULT_VLAN and VLAN-22, and ports A6 and A7 to belong only to VLAN-22, you would use the settings in figure page 2-27. (This example assumes the default GVRP setting—disabled—and that you do not plan to enable GVRP later.)

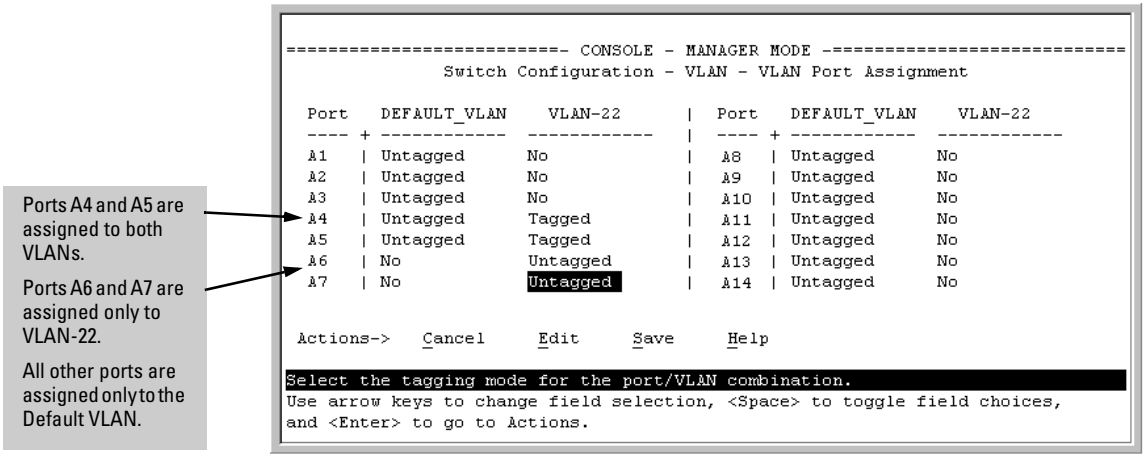

Ports A4 and A5 are assigned to both VLANs.
Ports A6 and A7 are assigned only to VLAN-22.
All other ports are assigned only to the Default VLAN.
========== CONSOLE - MANAGER MODE ==========
Switch Configuration - VLAN - VLAN Port Assignment
Port DEFAULT_VLAN VLAN-22 | Port DEFAULT_VLAN VLAN-22
A1 | Untagged No | A8 | Untagged No
A2 | Untagged No | A9 | Untagged No
A3 | Untagged No | A10 | Untagged No
A4 | Untagged Tagged | A11 | Untagged No
A5 | Untagged Tagged | A12 | Untagged No
A6 | No Untagged | A13 | Untagged No
A7 | No Untagged | A14 | Untagged No
Actions-> Cancel Edit Save Help
Select the tagging mode for the port/VLAN combination.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

Figure 2-17. Example of Port-Based VLAN Assignments for Specific Ports

For information on VLAN tags ("Untagged" and "Tagged"), refer to "802.1Q VLAN Tagging" on page 2-40.

d. If you are finished assigning ports to VLANs, press **[Enter]** and then **[S]** (for **Save**) to activate the changes you've made and to return to the Configuration menu. (The console then returns to the VLAN menu.)

3. Return to the Main menu.

CLI: Configuring Port-Based and Protocol-Based VLAN Parameters

In the factory default state, all ports on the switch belong to the (port-based) default VLAN (DEFAULT_VLAN; VID = 1) and are in the same broadcast/multicast domain. (The default VLAN is also the Primary VLAN. For more on this topic, refer to "The Primary VLAN" on page 2-45.) You can configure up to 255 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 256 (vids numbered up to 4094) VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP. Refer to chapter 3, "GVRP" .) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See "802.1Q VLAN Tagging" on page 2-40.)

VLAN Commands	Page
show vlans	below
show vlans < *vid* >	2-32
show vlans ports <*port-list*>	
max-vlans <1-256>	2-33
primary-vlan < *vid* >	2-34
[no] vlan < *vid* >	2-35
auto < *port-list* >	2-37 (Available if GVRP enabled.)
forbid	2-37
name < *vlan-name* >	2-37
protocol < *protocol-list* >	2-35
tagged < *port-list* >	2-37
untagged < *port-list* >	2-37
voice	2-54
static-vlan < *vlan-id* >	2-37 (Available if GVRP enabled.)

Displaying the Switch's VLAN Configuration. The **show vlans** command lists the VLANs currently running in the switch, with VID, VLAN name, and VLAN status. Dynamic VLANs appear only if the switch is running with GVRP enabled and one or more ports has dynamically joined an advertised VLAN. (In the default configuration, GVRP is disabled. (Refer to chapter 3, "GVRP" .)

Syntax: show vlans

Maximum VLANs to support: *Shows the number of VLANs the switch can currently support. (Default: 256 Maximum: 256)*

Primary VLAN: *Refer to "The Primary VLAN" on page 2-45.*

Management VLAN: *Refer to "The Secure Management VLAN" on page 2-46.*

802.1Q VLAN ID: *The VLAN identification number, or VID. Refer to "Terminology" on page 2-6.*

Name: *The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of* **VLAN-*x*** *where "**x**" matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of* **GVRP_*x*** *where "**x**" matches the applicable VID.*

Status:

Port-Based*: Port-Based, static VLAN*

Protocol: *Protocol-Based, static VLAN*

Dynamic: *Port-Based, temporary VLAN learned through GVRP (Refer to chapter 3, "GVRP" .)*

Voice: *Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to "Voice VLANs" on page 2-54.*

Jumbo: *Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled "Port Traffic Controls" in the* Management and Configuration Guide *for your switch.*

For example:

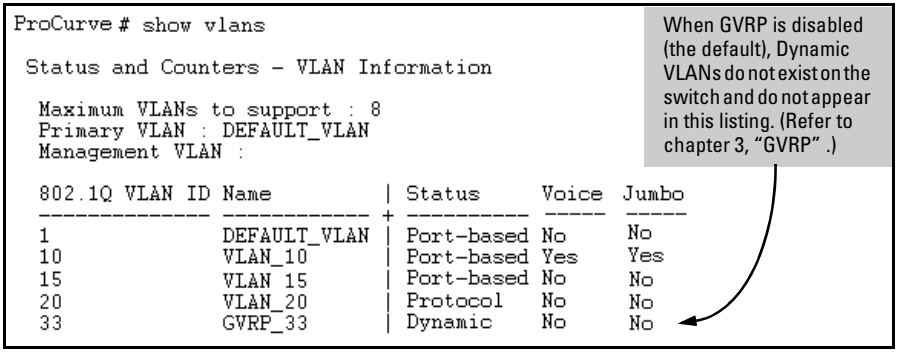

ProCurve # show vlans
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
Management VLAN :
802.1Q VLAN ID Name | Status Voice Jumbo
1 DEFAULT_VLAN | Port-based No No
10 VLAN_10 | Port-based Yes Yes
15 VLAN 15 | Port-based No No
20 VLAN_20 | Protocol No No
33 GVRP_33 | Dynamic No No
When GVRP is disabled (the default), Dynamic VLANs do not exist on the switch and do not appear in this listing. (Refer to chapter 3, "GVRP" .)

Figure 2-18. Example of "Show VLAN" Listing (GVRP Enabled)

Displaying the VLAN Membership of One or More Ports.

This command shows to which VLAN a port belongs.

Syntax: show vlan ports < *port-list* > [detail]

Displays VLAN information for an individual port or a group of ports, either cumulatively or on a detailed per-port basis.

port-list: *Specify a single port number, a range of ports (for example,* **a1-a16***), or* **all**.

detail: *Displays detailed VLAN membership information on a per-port basis.*

Descriptions of items displayed by the command are provided below.

Port name: *The user-specified port name, if one has been assigned.*

VLAN ID: *The VLAN identification number, or VID.*

Name: *The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of* **VLAN-*x*** *where "**x**" matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of* **GVRP_*x*** *where "**x**" matches the applicable VID.*

Status:

Port-Based*: Port-Based, static VLAN*

Protocol: *Protocol-Based, static VLAN*

Dynamic: *Port-Based, temporary VLAN learned through GVRP.*

Voice: *Indicates whether a (port-based) VLAN is configured as a voice VLAN.*

Jumbo: *Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled "Port Traffic Controls" in the* Management and Configuration Guide *for your switch.*

Mode: *Indicates whether a VLAN is tagged or untagged.*

Figure 2-19 is an example of the output when the **detail** option is not used.

```
ProCurve# show vlan ports a1-a33

Status and Counters - VLAN Information  - for ports
a1-a33

 802.1Q VLAN ID Name          | Status     Voice
 -------------- ------------ + ---------- -----
 1              DEFAULT_VLAN | Port-based No
 10             VLAN_10      | Port-based Yes
 15             VLAN 15      | Port-based No
 20             VLAN_20      | Protocol   No
 33             GVRP_33      | Dynamic    No
```

Figure 2-19. Example of "Show VLAN Ports" Cumulative Listing

Figure 2-20 is an example of the output when the **detail** option is used.

```
ProCurve# show vlan ports a1-a4 detail

 Status and Counters - VLAN Information - for ports A1

  Port name: Voice_Port
  VLAN ID  Name               | Status     Voice Jumbo Mode
  -------  ------------------ + ---------- ----- ----- ------
  1        DEFAULT_VLAN       | Port-based No    No    Untagged
  10       VLAN_10            | Port-based Yes   No    Tagged

 Status and Counters - VLAN Information - for ports A2

  Port name: Uplink_Port
  VLAN ID  Name               | Status     Voice Jumbo Mode
  -------  ------------------ + ---------- ----- ----- ------
  1        DEFAULT_VLAN       | Port-based No    No    Untagged
  20       VLAN_20            | Protocol   No    No    Tagged
  33       GVRP_33            | Dynamic    No    No    Tagged

 Status and Counters - VLAN Information - for ports A3

  VLAN ID  Name               | Status     Voice Jumbo Mode
  -------  ------------------ + ---------- ----- ----- ------
  1        DEFAULT_VLAN       | Port-based No    No    Untagged

 Status and Counters - VLAN Information - for ports A4

  VLAN ID  Name               | Status     Voice Jumbo Mode
  -------  ------------------ + ---------- ----- ----- ------
  1        DEFAULT_VLAN       | Port-based No    No    Untagged
```

Figure 2-20. Example of "Show VLAN Ports" Detail Listing

Displaying the Configuration for a Particular VLAN . This command uses the VID to identify and display the data for a specific static or dynamic VLAN.

Syntax: show vlans < *vlan-id* >

802.1Q VLAN ID: *The VLAN identification number, or VID. Refer to "Terminology" on page 2-6.*

Name: *The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of* **VLAN-*x*** *where "**x**" matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of* **GVRP_*x*** *where "**x**" matches the applicable VID.*

Status:

Port-Based*: Port-Based, static VLAN*

Protocol: *Protocol-Based, static VLAN*

Dynamic: *Port-Based, temporary VLAN learned through GVRP (Refer to chapter 3,"GVRP" in this guide.)*

Voice: *Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to "Voice VLANs" on page 2-54.*

Jumbo: *Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled "Port Traffic Controls" in the* Management and Configuration Guide *for your switch.*

Port Information: *Lists the ports configured as members of the VLAN.*

DEFAULT: *Shows whether a port is a tagged or untagged member of the listed VLAN.*

Unknown VLAN: *Shows whether the port can become a dynamic member of an unknown VLAN for which it receives an advertisement. GVRP must be enabled to allow dynamic joining to occur. Refer to table 3-1 on page 3-8.*

Status: *Shows whether the port is participating in an active link.*

```
ProCurve(config)# show vlans 22
 Status and Counters - VLAN Information - Ports - VLAN 22
  802.1Q VLAN ID : 22
  Name : VLAN22
  Status : Port-based
  Voice : Yes
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A12              Untagged Learn        Up
  A13              Untagged Learn        Up
  A14              Untagged Learn        Up
  A15              Untagged Learn        Down
  A16              Untagged Learn        Up
  A17              Untagged Learn        Up
  A18              Untagged Learn        Up
```

Figure 2-21. Example of "Show VLAN" for a Specific Static VLAN

Show VLAN lists this data when GVRP is enabled and at least one port on the switch has dynamically joined the designated VLAN.

```
ProCurve# show vlans 33
 Status and Counters - VLAN Information - Ports - VLAN 33

  802.1Q VLAN ID : 33
  Name : GVRP_33
  Status : Dynamic
  Voice : No
  Jumbo : No
  Port Information DEFAULT  Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A6               Auto     Learn        Up
```

Figure 2-22. Example of "Show VLAN" for a Specific Dynamic VLAN

Changing the Number of VLANs Allowed on the Switch. In the default VLAN configuration, the switch allows a maximum of 256 VLANs. You can specify any value from 1 to 256.

Syntax: max-vlans < 1-256 >

Specifies the maximum number of VLANs to allow. (If GVRP is enabled, this setting includes any dynamic VLANs on the switch.) As part of implementing a new setting, you must execute a **write memory** *command (to save the new value to the startup-config file) and then reboot the switch.*

Note: *If multiple VLANs exist on the switch, you cannot reset the maximum number of VLANs to a value smaller than the current number of VLANs.*

For example, to reconfigure the switch to allow 10 VLANs:

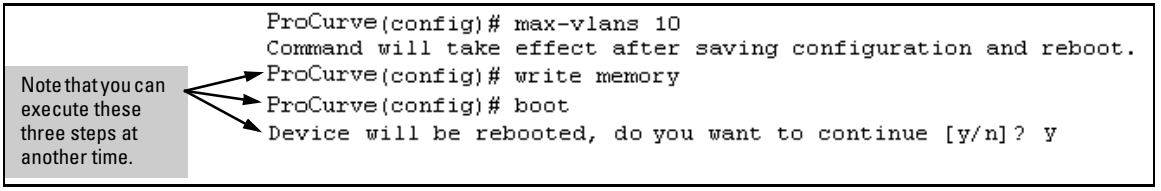

ProCurve(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
ProCurve(config)# write memory
ProCurve(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
Note that you can execute these three steps at another time.

Figure 2-23. Example of Command Sequence for Changing the Number of VLANs

Changing the Primary VLAN. In the default VLAN configuration, the port-based default VLAN (**DEFAULT_VLAN**) is the Primary VLAN. However, you can reassign the Primary VLAN to any port-based, static VLAN on the switch. (For more on the Primary VLAN, refer to "The Primary VLAN" on page 2-45.) To identify the current Primary VLAN and list the available VLANs and their respective VIDs, use **show vlans**.

Syntax: primary-vlan < *vid* | *ascii-name-string* >

Reassigns the Primary VLAN function. Re-assignment must be to an existing, port-based, static VLAN. (The switch will not reassign the Primary VLAN function to a protocol VLAN.) If you re-assign the Primary VLAN to a non-default VLAN, you cannot later delete that VLAN from the switch until you again re-assign the Primary VLAN to another port-based, static VLAN.

For example, if you wanted to reassign the Primary VLAN to VLAN 22 and rename the VLAN with "22-Primary" and display the result:

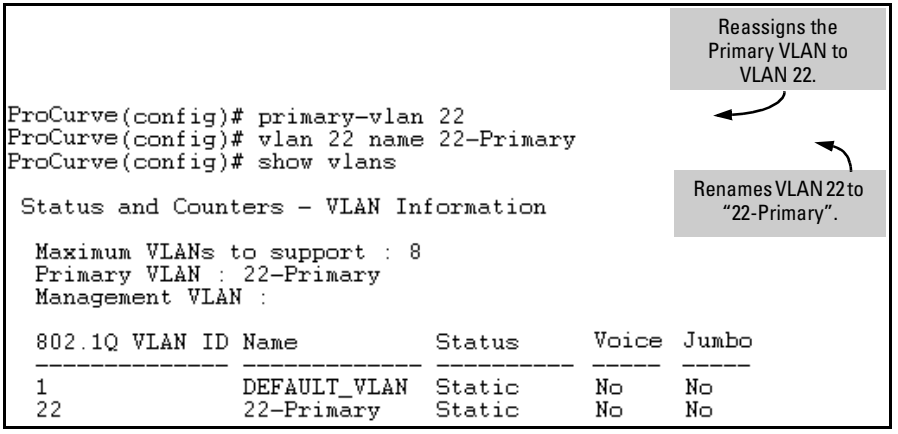

Reassigns the Primary VLAN to VLAN 22.
Renames VLAN 22 to "22-Primary".
ProCurve(config)# primary-vlan 22
ProCurve(config)# vlan 22 name 22-Primary
ProCurve(config)# show vlans
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : 22-Primary
Management VLAN :
802.1Q VLAN ID Name Status Voice Jumbo
1 DEFAULT_VLAN Static No No
22 22-Primary Static No No

Figure 2-24. Example of Reassigning Primary VLAN and Changing the VLAN Name

Creating a New Static VLAN (Port-Based or Protocol-Based)
Changing the VLAN Context Level. The **vlan < *vid*>** command operates in the global configuration context to either configure a static VLAN and/or take the CLI to the specified VLAN's context.

Syntax: vlan < *vid* | *ascii-name-string* >
[no] vlan < *vid* >

If < vid > does not exist in the switch, this command creates a port-based VLAN with the specified < vid >. If the command does not include options, the CLI moves to the newly created VLAN context. If you do not specify an optional name, the switch assigns a name in the default format: **VLAN*n*** *where* ***n*** *is the < vid > assigned to the VLAN. If the VLAN already exists and you enter either the* ***vid*** *or the* ***ascii-name-string****, the CLI moves to the specified VLAN's context.*

The **[no]** *form of the command deletes the VLAN as follows:*

- *If one or more ports belong only to the VLAN to be deleted, the CLI notifies you that these ports will be moved to the default VLAN and prompts you to continue the deletion. For member ports that also belong to another VLAN, there is no "move" prompt.*

[protocol < ipx | ipv4 | ipv6 | arp | appletalk | sna | netbeui >]

Configures a static, protocol VLAN of the specified type. If multiple protocols are configured in the VLAN, then the **[no]** *form removes the specified protocol from the VLAN. If a protocol VLAN is configured with only one protocol type and you use the* **[no]** *form of this command to remove that protocol, the switch changes the protocol VLAN to a port-based VLAN if the VLAN does not have an untagged member port. (If an untagged member port exists on the protocol VLAN, you must either convert the port to a tagged member or remove the port from the VLAN before removing the last protocol type from the VLAN.)*

Note: *If you create an IPv4 protocol VLAN, you must also assign the ARP protocol option to the VLAN to provide IP address resolution. Otherwise, IP packets are not deliverable. A "Caution" message appears in the CLI if you configure IPv4 in protocol VLAN that does not already include the arp protocol option. The same message appears if you add or delete another protocol in the same VLAN.*

name < *ascii-name-string* >

When included in a **vlan** *command for creating a new static VLAN, specifies a non-default VLAN name. Also used to change the current name of an existing VLAN. (Avoid spaces and the following characters in the <* ***ascii-name-string*** *> entry:* **@**, **#**, **$**, **^**, **&**, *****, **(**, and **)**. *To include a blank space in a VLAN name, enclose the name in single or double quotes ('...' or "...").*

[voice]

Designates a VLAN for VoIP use. For more on this topic, refer to "Voice VLANs" on page 2-54.

For example, to create a new, port-based, static VLAN with a VID of 100:

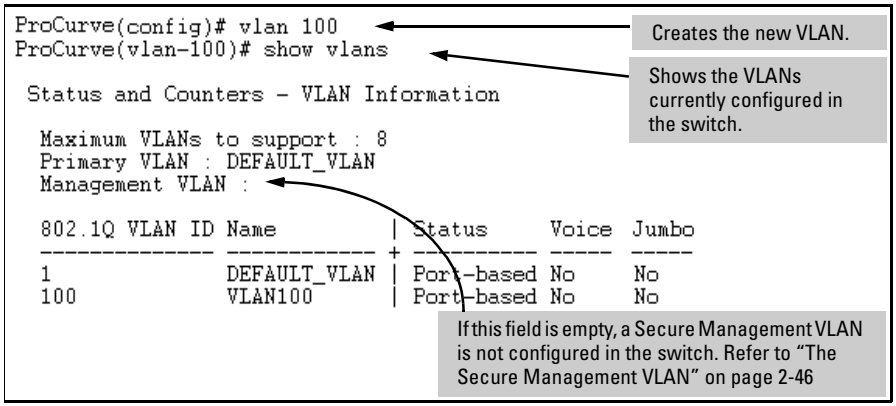

ProCurve(config)# vlan 100
ProCurve(vlan-100)# show vlans
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
Management VLAN :
802.1Q VLAN ID Name | Status Voice Jumbo
1 DEFAULT_VLAN | Port-based No No
100 VLAN100 | Port-based No No
Creates the new VLAN.
Shows the VLANs currently configured in the switch.
If this field is empty, a Secure Management VLAN is not configured in the switch. Refer to "The Secure Management VLAN" on page 2-46

Figure 2-25. Example of Creating a New, Port-Based, Static VLAN

To go to a different VLAN context level, such as to the default VLAN:

```
ProCurve(vlan-100)# vlan default_vlan
ProCurve(vlan-1) _
```

Deleting a VLAN. If ports B1-B5 belong to both VLAN 2 and VLAN 3, and ports B6-B10 belong to VLAN 3 only, then deleting VLAN 3 causes the CLI to prompt you to approve moving ports B6 - B10 to VLAN 1 (the default VLAN). (Ports B1-B5 are not moved because they still belong to another VLAN.)

```
ProCurve(config)# no vlan 3
The following ports will be moved to the default VLAN:
B6-B10
Do you want to continue? [y/n] y
ProCurve(config)#
```

Converting a Dynamic VLAN to a Static VLAN. Use this feature if you want to convert a dynamic, port-based VLAN membership to a static, port-based VLAN membership. This is necessary if you want to make the VLAN permanent on the switch.

Syntax: static-vlan < *vlan-id* >

Converts a dynamic, port-based VLAN membership to a static, port-based VLAN membership. (Allows port-based VLANs only). For this command, < *vlan-id* > *refers to the VID of the dynamic VLAN membership. (Use* **show vlan** to help identify the VID you need to use.) *This command requires that GVRP is running on the switch and a port is currently a dynamic member of the selected VLAN. After you convert a dynamic VLAN to static, you must configure the switch's per-port participation in the VLAN in the same way that you would for any static VLAN. (For GVRP and dynamic VLAN operation, refer to chapter 3, "GVRP" .)*

For example, suppose a dynamic VLAN with a VID of 125 exists on the switch. The following command converts the VLAN to a port-based, static VLAN.

```
ProCurve(config)# static-vlan 125
```

Configuring Static VLAN Per-Port Settings. The **vlan <***vlan-id***>** command, used with the options listed below, changes the name of an existing static VLAN and changes the per-port VLAN membership settings.

Note

You can use these options from the configuration level by beginning the command with **vlan <** *vid* **>**, or from the context level of the specific VLAN by just typing the command option.

Syntax: [no] vlan < *vid* >

tagged < *port-list* >

Configures the indicated port(s) as **Tagged** *for the specified VLAN. The "***no***" version sets the port(s) to either* **No** *or (if GVRP is enabled) to* **Auto**.

untagged < *port-list* >

Configures the indicated port(s) as **Untagged** *for the specified VLAN. The "***no***" version sets the port(s) to either* **No** *or (if GVRP is enabled) to* **Auto**.

forbid < *port-list* >

Used in port-based VLANs to configures **<** *port-list* **>** *as "forbidden" to become a member of the specified VLAN, as well as other actions. Does not operate with protocol VLANs. The "***no***" version sets the port(s) to either* **No** *or (if GVRP is enabled) to* **Auto**. *Refer to chapter 3, "GVRP", in this guide.*

auto < *port-list* >

Available if GVRP is enabled on the switch. Returns the per-port settings for the specified VLAN to **Auto** *operation. Note that* **Auto** *is the default per-port setting for a static VLAN if GVRP is running on the switch.* (For information on dynamic VLAN and GVRP operation, refer to *chapter 3, "GVRP", in this guide.*)

For example, suppose you have a VLAN named VLAN100 with a VID of 100, and all ports are set to **No** for this VLAN. To change the VLAN name to "**Blue_Team**" and set ports A1 - A5 to **Tagged**, you would use these commands:

```
ProCurve(config)# vlan 100 name Blue_Team
ProCurve(config)# vlan 100 tagged a1-a5
```

To move to the vlan 100 context level and execute the same commands:

```
ProCurve(config)# vlan 100
ProCurve(vlan-100)# name Blue_Team
ProCurve(vlan-100)# tagged a1-a5
```

Similarly, to change the tagged ports in the above examples to **No** (or **Auto**, if GVRP is enabled), you could use either of the following commands.

At the global config level, use:

```
ProCurve(config)# no vlan 100 tagged a1-a5
```

- or -

At the VLAN 100 context level, use:

```
ProCurve(vlan-100)# no tagged a1-a5
```

Note

You cannot use these commands with dynamic VLANs. Attempting to do so results in the message "**VLAN already exists.**" and no change occurs.

Web: Viewing and Configuring VLAN Parameters

In the web browser interface you can do the following:

- Add VLANs
- Rename VLANs
- Remove VLANs
- Configure VLAN tagging mode per-port
- Configure GVRP mode
- Select a new Primary VLAN

To configure other static VLAN port parameters, you will need to use either the CLI or the menu interface (available by Telnet from the web browser interface).

1. Click on the Configuration tab.
2. Click on **[Vlan Configuration]**.
3. Click on **[Add/Remove VLANs]**.

For web-based Help on how to use the web browser interface screen, click on the **[?]** button provided on the web browser screen.

802.1Q VLAN Tagging

General Applications:

- The switch requires VLAN tagging on a given port if more than one VLAN of the same type uses the port. When a port belongs to two or more VLANs of the same type, they remain as separate broadcast domains and cannot receive traffic from each other without routing. (If multiple, *non-routable* VLANs exist in the switch—such as NETbeui protocol VLANs— then they cannot receive traffic from each other under any circumstances.)
- The switch requires VLAN tagging on a given port if the port will be receiving inbound, tagged VLAN traffic that should be forwarded. Even if the port belongs to only one VLAN, it forwards inbound tagged traffic only if it is a tagged member of that VLAN.
- If the only authorized, inbound VLAN traffic on a port arrives untagged, then the port must be an untagged member of that VLAN. This is the case where the port is connected to a non 802.1Q-compliant device or is assigned to only one VLAN.

For example, if port 7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain “untagged” because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port 7, then at least one of those VLAN assignments must be “tagged” so that Red VLAN traffic can be distinguished from Green VLAN traffic. Figure 2-26 shows this concept:

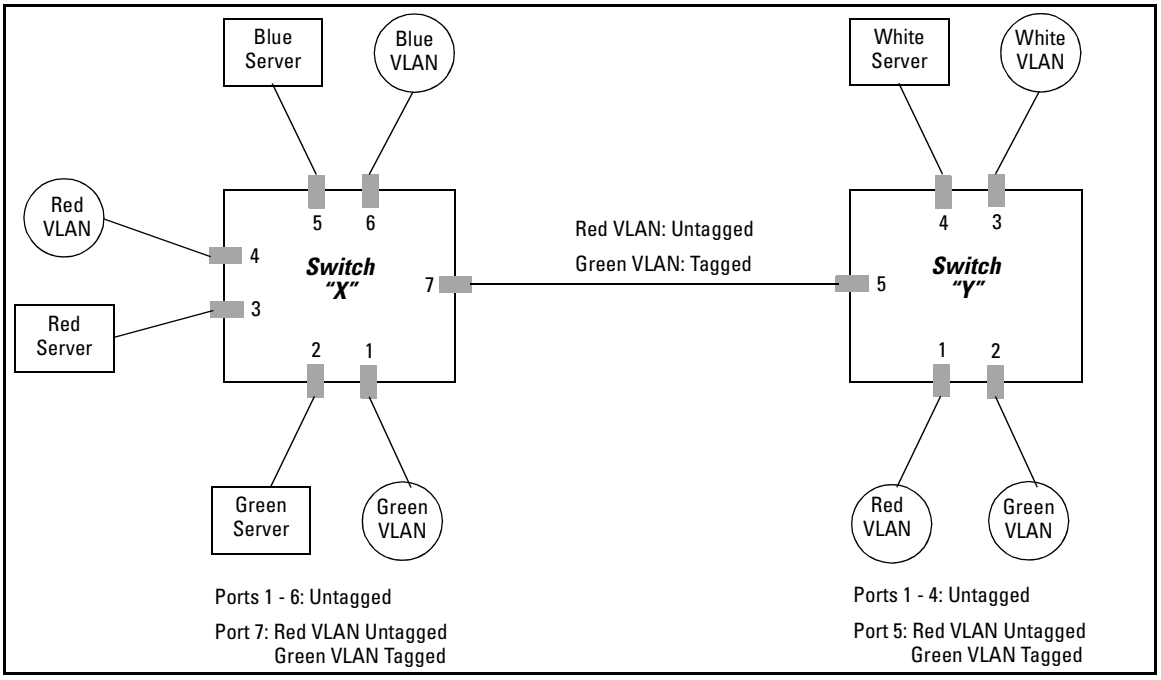


Figure 2-26. Example of Tagged and Untagged VLAN Port Assignments

- In switch X:
  - VLANs assigned to ports X1 - X6 can all be untagged because there is only one VLAN assignment per port. Red VLAN traffic will go out only the Red ports; Green VLAN traffic will go out only the Green ports, and so on. Devices connected to these ports do not have to be 802.1Q-compliant.
  - However, because both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.
- In switch Y:
  - VLANs assigned to ports Y1 - Y4 can all be untagged because there is only one VLAN assignment per port. Devices connected to these ports do not have to be 802.1Q-compliant.
  - Because both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port.
- In both switches: The ports on the link between the two switches must be configured the same. As shown in figure 2-26 (above), the Red VLAN must be untagged on port X7 and Y5 and the Green VLAN must be tagged on port X7 and Y5, or vice-versa.

Note

Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN *must* be given the same VID in every device in which it is configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be used for the Red VID in switch Y.

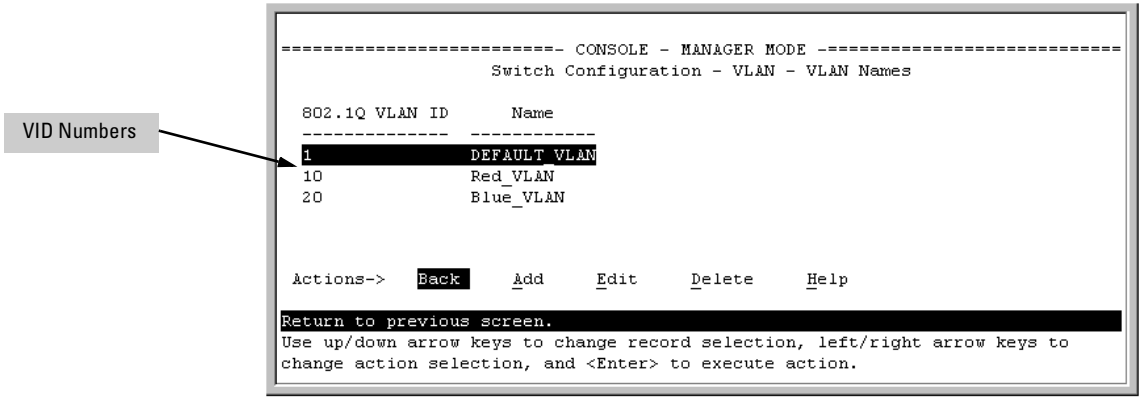

VID Numbers
========== CONSOLE - MANAGER MODE ==========
Switch Configuration - VLAN - VLAN Names
802.1Q VLAN ID
Name
1 DEFAULT_VLAN
10 Red_VLAN
20 Blue_VLAN
Actions-> Back Add Edit Delete Help
Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to change action selection, and <Enter> to execute action.

Figure 2-27. Example of VLAN ID Numbers Assigned in the VLAN Names Screen

VLAN tagging gives you several options:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as "Untagged" (the default) if the authorized inbound traffic for that port arrives untagged.
- Any port with two or more VLANs of the same type can have one such VLAN assigned as "Untagged". All other VLANs of the same type must be configured as "Tagged". That is:

Port-Based VLANs	Protocol VLANs
A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.	A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.
A port can be a tagged member of any port-based VLAN. See above.	A port can be a tagged member of any protocol-based VLAN. See above.
Note: A given VLAN ***must*** have the same VID on all 802.1Q-compliant devices in which the VLAN occurs. Also, the ports connecting two 802.1Q devices should have identical VLAN configurations.	

- If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, then, you can configure all VLAN assignments on a port as "Tagged" if doing so either makes it easier to manage your VLAN assignments, or if the authorized, inbound traffic for all VLANs on the port will be tagged.

For a summary and flowcharts of untagged and tagged VLAN operation on inbound traffic, refer to the following under "VLAN Operating Rules" on pages 2-13 through 2-16:

- "Inbound Tagged Packets"
- "Untagged Packet Forwarding" and figure 2-7
- "Tagged Packet Forwarding" and figure 2-8

Example. In the following network, switches X and Y and servers S1, S2, and the AppleTalk server are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.) This network includes both protocol-based (AppleTalk) VLANs and port-based VLANs.

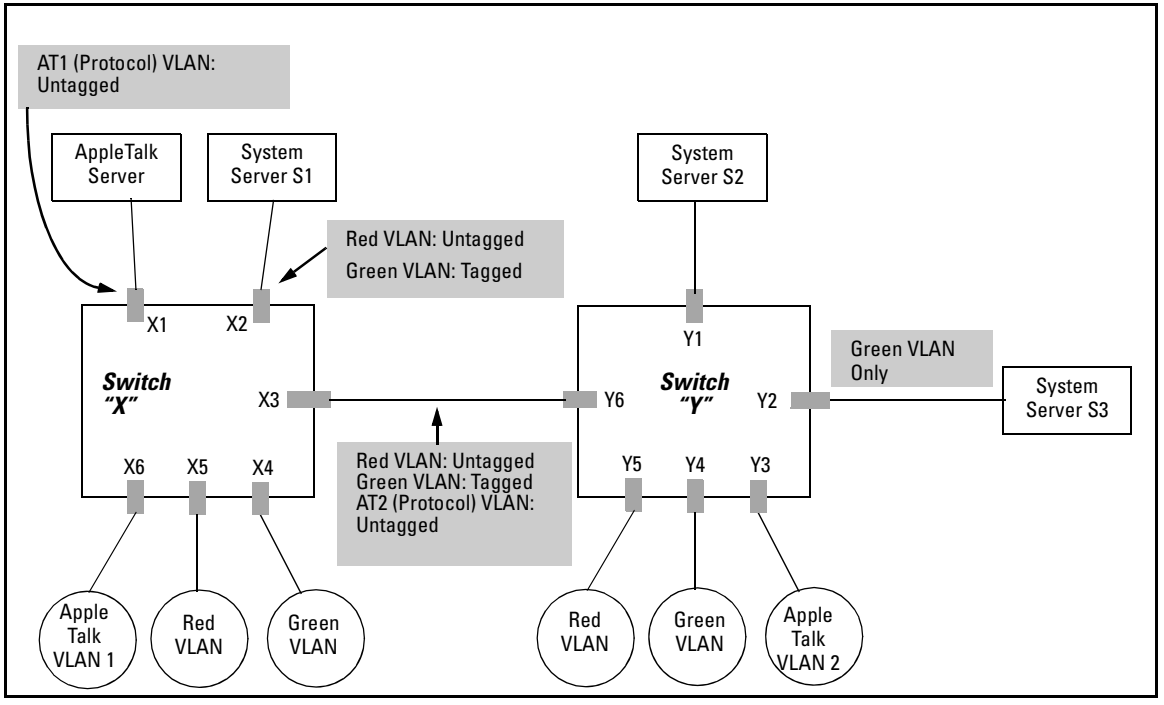


Figure 2-28. Example of Networked 802.1Q-Compliant Devices with Multiple VLANs on Some Ports

- The VLANs assigned to ports X4 - X6, Y2 - Y5 can all be untagged because there is only one VLAN assigned per port.
- Port X1 has two AppleTalk VLANs assigned, which means that one VLAN assigned to this port can be untagged and the other must be tagged.
- Ports X2 and Y1 have two port-based VLANs assigned, so one can be untagged and the other must be tagged on both ports.
- Ports X3 and Y6 have two port-based VLANs and one protocol-based VLAN assigned. Thus, one port-based VLAN assigned to this port can be untagged and the other must be tagged. Also, since these two ports share the same link, their VLAN configurations must match.

Switch X					***Switch Y***				
Port	**AT-1 VLAN**	**AT-2 VLAN**	**Red VLAN**	**Green VLAN**	**Port**	**AT-1 VLAN**	**AT-2 VLAN**	**Red VLAN**	**Green VLAN**
X1	Untagged	Tagged	No*	No*	Y1	No*	No*	Untagged	Tagged
X2	No*	No*	Untagged	Tagged	Y2	No*	No*	No*	Untagged
X3	No*	Untagged	Untagged	Tagged	Y3	No*	Untagged	No*	No*
X4	No*	No*	No*	Untagged	Y4	No*	No*	No*	Untagged
X5	No*	No*	Untagged	No*	Y5	No*	No*	Untagged	No*
X6	Untagged	No*	No*	No*	Y6	No	Untagged	Untagged	Tagged

*"No" means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic. Also, if GVRP were enabled (port-based only), "Auto" would appear instead of "No".

Note

VLAN configurations on ports connected by the same link must match. Because ports X2 and Y5 are opposite ends of the same point-to-point connection, both ports must have the same VLAN configuration; that is, both ports configure the Red VLAN as "Untagged" and the Green VLAN as "Tagged".

Special VLAN Types

VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the port-based, default VLAN (named DEFAULT_VLAN). This places all ports in the switch into one physical broadcast domain. In the factory-default state, the default VLAN is also the *Primary* VLAN.

You can partition the switch into multiple virtual broadcast domains by configuring one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 256 (vids numbered up to 4094) static and dynamic VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN's VID (which is always "1"). Although you can remove all ports from the default VLAN (by placing them in another port-based VLAN), this VLAN is always present; that is, you cannot delete it from the switch.

For details on port VLAN settings, refer to "Configuring Static VLAN Per-Port Settings" on page 2-37

The Primary VLAN

Because certain features and management functions run on only one VLAN in the switch, and because DHCP and Bootp can run per-VLAN, there is a need for a dedicated VLAN to manage these features and ensure that multiple instances of DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch. The *Primary* VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch designates the default VLAN (DEFAULT_VLAN; VID = 1) as the Primary VLAN. However, to provide more control in your network, you can designate another static, port-based VLAN as primary. To summarize, *designating a non-default VLAN as primary* means that:

- The switch reads DHCP responses on the Primary VLAN instead of on the default VLAN. (This includes such DHCP-resolved parameters as the TimeP server address, Default TTL, and IP addressing—including the Gateway IP address—when the switch configuration specifies DHCP as the source for these values.)
- The default VLAN continues to operate as a standard VLAN (except, as noted above, you cannot delete it or change its VID).

- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether it is the Primary VLAN.

Candidates for Primary VLAN include any static, port-based VLAN currently configured on the switch. (Protocol-Based VLANs and dynamic—GVRP-learned—VLANs that have not been converted to a static VLAN cannot be the Primary VLAN.) To display the current Primary VLAN, use the CLI **show vlan** command.

Note

If you configure a non-default VLAN as the Primary VLAN, you cannot delete that VLAN unless you first select a different VLAN to serve as primary.

If you manually configure a gateway on the switch, it ignores any gateway address received via DHCP or Bootp.

To change the Primary VLAN configuration, refer to "Changing the Primary VLAN" on page 2-34.

The Secure Management VLAN

Configuring a secure Management VLAN creates an isolated network for managing the ProCurve switches that support this feature. If you configure a secure Management VLAN, access to the VLAN and to the switch's management functions (Menu, CLI, and web browser interface) is available only through ports configured as members.

- Multiple ports on the switch can belong to the Management VLAN. This allows connections for multiple management stations you want to have access to the Management VLAN, while at the same time allowing Management VLAN links between switches configured for the same Management VLAN.
- Only traffic from the Management VLAN can manage the switch, which means that only the workstations and PCs connected to ports belonging to the Management VLAN can manage and reconfigure the switch.

Figure 2-29 illustrates use of the Management VLAN feature to support management access by a group of management workstations.

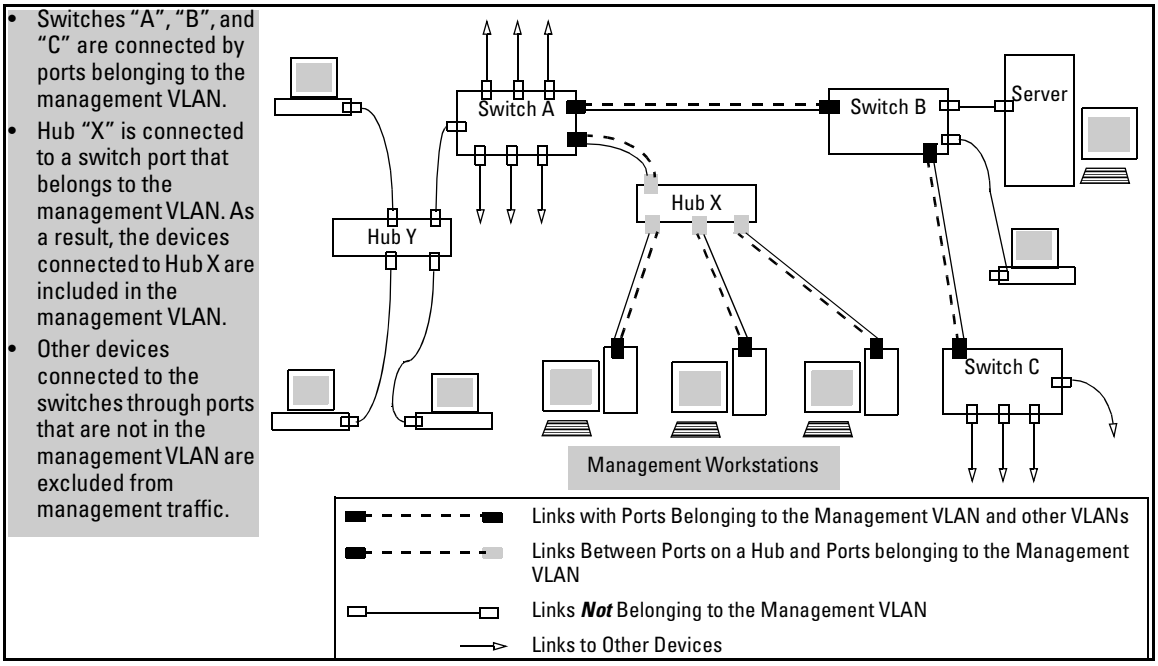

• Switches "A", "B", and "C" are connected by ports belonging to the management VLAN.
• Hub "X" is connected to a switch port that belongs to the management VLAN. As a result, the devices connected to Hub X are included in the management VLAN.
• Other devices connected to the switches through ports that are not in the management VLAN are excluded from management traffic.
Switch A
Switch B
Server
Hub X
Hub Y
Switch C
Management Workstations
Links with Ports Belonging to the Management VLAN and other VLANs
Links Between Ports on a Hub and Ports belonging to the Management VLAN
Links *Not* Belonging to the Management VLAN
Links to Other Devices

Figure 2-29. Example of Potential Security Breaches

In figure 2-30, Workstation 1 has management access to all three switches through the Management VLAN, while the PCs do not. This is because configuring a switch to recognize a Management VLAN automatically excludes attempts to send management traffic from any other VLAN.

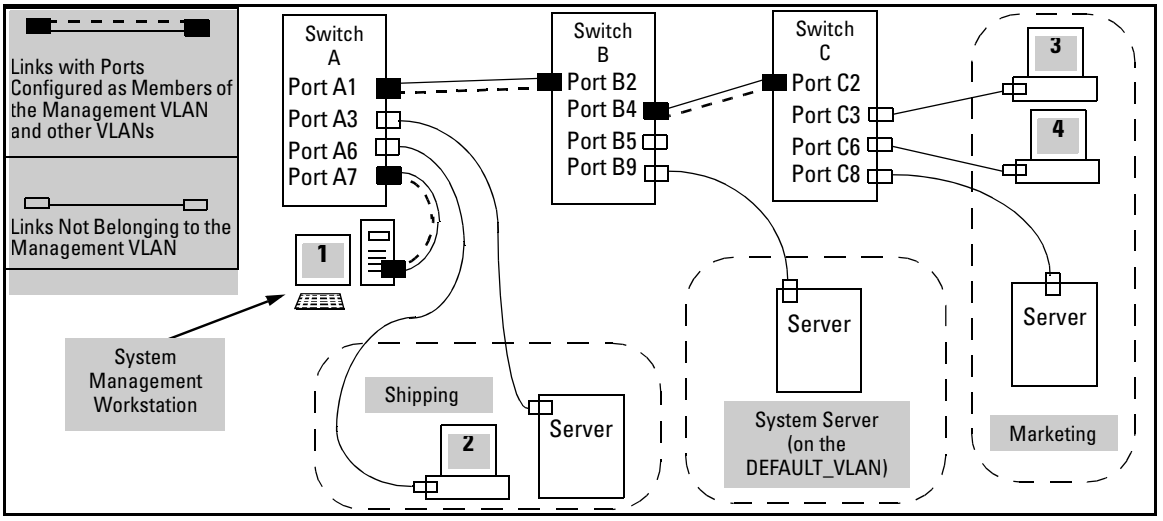


Figure 2-30. Example of Management VLAN Control in a LAN

Table 2-5. VLAN Membership in Figure 2-30

Switch	A1	A3	A6	A7	B2	B4	B5	B9	C2	C3	C6	C8
Management VLAN (VID = 7)	**Y**	N	N	**Y**	**Y**	**Y**	N	N	**Y**	N	N	N
Marketing VLAN (VID = 12)	N	N	N	N	N	N	N	N	N	**Y**	**Y**	**Y**
Shipping Dept. VLAN (VID = 20)	N	**Y**	**Y**	N	N	N	N	N	N	N	N	N
DEFAULT-VLAN (VID = 1)	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

Preparation

1. Determine a VID and VLAN name suitable for your Management VLAN.
2. Plan your Management VLAN topology to use ProCurve switches that support this feature. (Refer to page 2-46.) The ports belonging to the Management VLAN should be only the following:
   - Ports to which you will connect authorized management stations (such as Port A7 in figure 2-30.)
   - Ports on one switch that you will use to extend the Management VLAN to ports on other ProCurve switches (such as ports A1 and B2 or B4 and C2 in figure 2-30 on page 2-48.).

Hubs dedicated to connecting management stations to the Management VLAN can also be included in the above topology. Note that any device connected to a hub in the Management VLAN will also have Management VLAN access.

3. Configure the Management VLAN on the selected switch ports.

4. Test the management VLAN from all of the management stations authorized to use the Management VLAN, including any SNMP-based network management stations. Ensure that you include testing any Management VLAN links between switches.

Note

If you configure a Management VLAN on a switch by using a Telnet connection through a port that is not in the Management VLAN, then you will lose management contact with the switch if you log off your Telnet connection or execute **write memory** and **reboot** the switch.

Configuration

Note

In order to enable management-vlan, oobm must be disabled first, since the two are mutually exclusive.

Syntax: [no] management-vlan < *vlan-id* / *vlan-name* >

Configures an existing VLAN as the management VLAN. The **no** *form disables the management VLAN and returns the switch to its default management operation. Default: Disabled. In this case, the VLAN returns to standard VLAN operation.*

For example, suppose you have already configured a VLAN named **My_VLAN** with a VID of 100. Now you want to configure the switch to do the following:

- Use **My_VLAN** as a Management VLAN (tagged, in this case) to connect port A1 on switch "A" to a management station. (The management station includes a network interface card with 802.1Q tagged VLAN capability.)
- Use port A2 to extend the Management VLAN to port B1 (which is already configured as a tagged member of **My_VLAN**) on an adjacent Procurve switch that supports the Management VLAN feature.

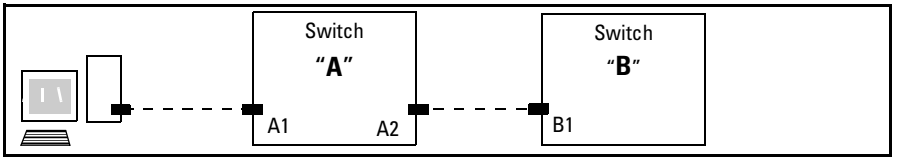


Figure 2-31. Illustration of Configuration Example

```
ProCurve (config)# management-vlan 100
ProCurve (config)# vlan 100 tagged a1
ProCurve (config)# vlan 100 tagged a2
```

Using DHCP to Obtain an IP Address

You can use DHCP to obtain an IPv4 address for your Management VLAN or a client on that VLAN. The following examples illustrate when an IP address will be received from the DHCP server.

1. If Blue_VLAN is configured as the Management VLAN and the DHCP server is also on Blue_VLAN, Blue_VLAN receives an IP address. Because DHCP Relay does not forward onto or off of the Management VLAN, devices on Red_VLAN cannot get an IP address from the DHCP server on Blue_VLAN (Management VLAN) and Red_VLAN does not receive an IP address. See figure 2-32.

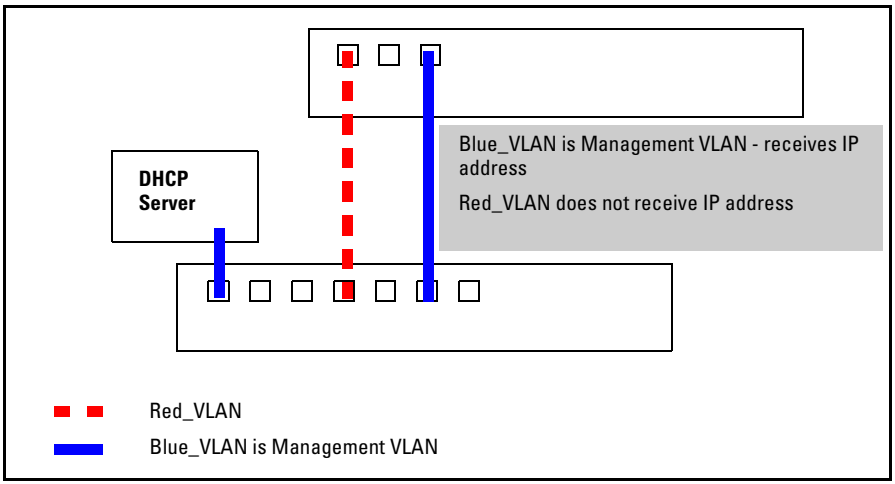


Figure 2-32. Example of DHCP Server on Management VLAN

2. If Red_VLAN is configured as the Management VLAN and the DHCP server is on Blue_VLAN, Blue_VLAN receives an IP address but Red_VLAN does not. See figure 2-33.

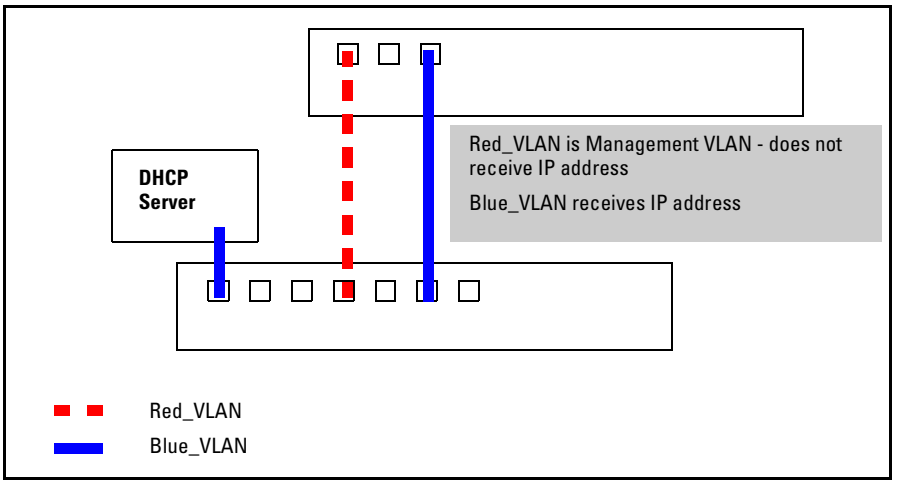


Figure 2-33. Example of DHCP Server on Different VLAN from the Management VLAN

3. If no Management VLAN is configured, both Blue_VLAN and Red_VLAN receive IP addresses. See figure 2-34.

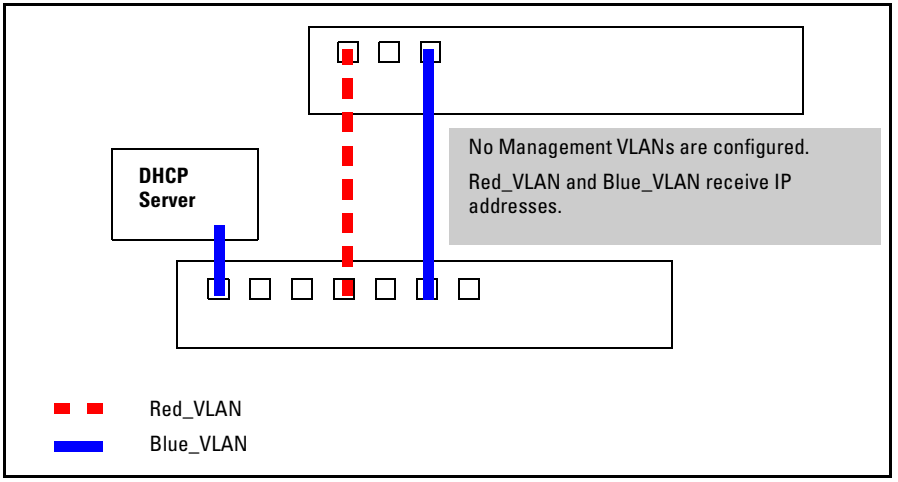


Figure 2-34. Example of no Management VLANs Configured

4. If Red_VLAN is configured as the Management VLAN and the client is on Red_VLAN, but the DHCP server is on Blue_VLAN, the client will not receive an IP address. See figure 2-35.

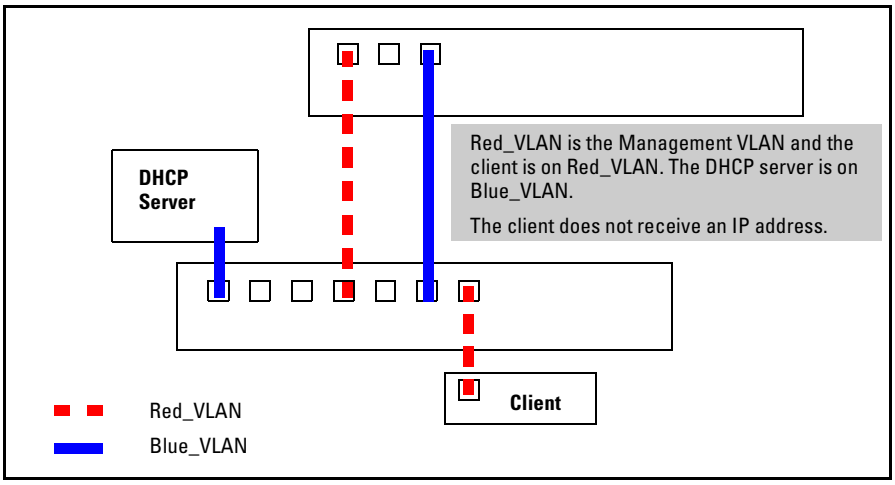

DHCP
Server
Red_VLAN is the Management VLAN and the client is on Red_VLAN. The DHCP server is on Blue_VLAN.
The client does not receive an IP address.
Client
Red_VLAN
Blue_VLAN

Figure 2-35. Example of Client on Different Management VLAN from DHCP Server

5. If Blue_VLAN is configured as the Management VLAN, the client is on Blue_VLAN, and the DHCP server is on Blue_VLAN, the client receives an IP address.

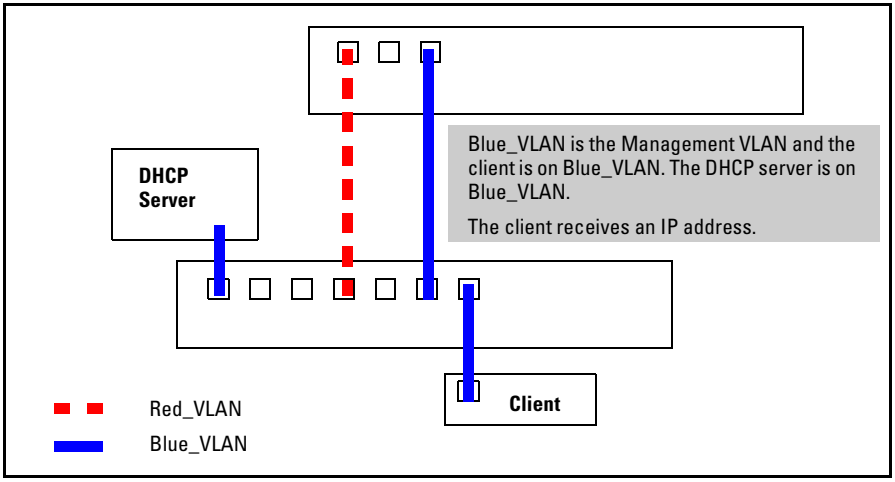

DHCP
Server
Blue_VLAN is the Management VLAN and the client is on Blue_VLAN. The DHCP server is on Blue_VLAN.
The client receives an IP address.
Client
Red_VLAN
Blue_VLAN

Figure 2-36. Example of DHCP Server and Client on the Management VLAN

Deleting the Management VLAN

You can disable the Secure Management feature without deleting the VLAN itself. For example, either of the following commands disables the Secure Management feature in the above example:

```
ProCurve (config)# no management-vlan 100
ProCurve (config)# no management-vlan my_vlan
```

Operating Notes for Management VLANs

- Use only a static, port-based VLAN for the Management VLAN.
- The Management VLAN feature applies to both IPv4 and IPv6 traffic.
- The Management VLAN does not support IGMP operation.
- Routing between the Management VLAN and other VLANs is not allowed.
- If there are more than 25 VLANs configured on the switch, reboot the switch after configuring the management VLAN.
- If you implement a Management VLAN in a switch mesh environment, all meshed ports on the switch will be members of the Management VLAN.
- Only one Management-VLAN can be active in the switch. If one Management-VLAN VID is saved in the startup-config file and you configure a different VID in the running-config file, the switch uses the running-config version until you either use the **write-memory** command or reboot the switch.
- During a Telnet session to the switch, if you configure the Management-VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you terminate the session by logging out or rebooting the switch.
- During a web browser session to the switch, if you configure the Management-VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you close the browser session or rebooting the switch.

Note

The Management-VLAN feature does not control management access through a direct connection to the switch's serial port.

- Enabling Spanning Tree where there are multiple links using separate VLANs, including the Management VLAN, between a pair of switches, Spanning Tree will force the blocking of one or more links. This may include the link carrying the Management VLAN, which will cause loss of management access to some devices. This can also occur where meshing is configured and the Management VLAN is configured on a separate link.

- Monitoring Shared Resources: The Management VLAN feature shares internal switch resources with several other features. The switch provides ample resources for all features. However, if the internal resources become fully subscribed, the Management VLAN feature cannot be configured until the necessary resources are released from other uses. For information on determining the current resource availability and usage, refer to the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.

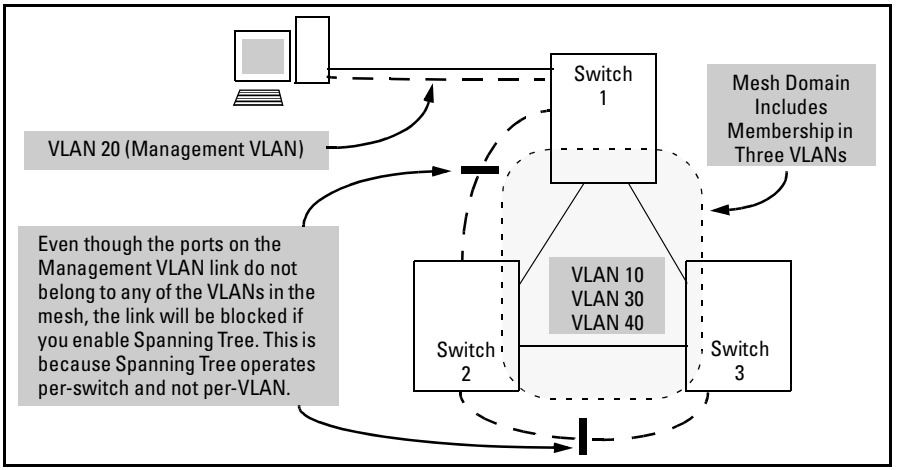

Switch 1
Mesh Domain Includes Membership in Three VLANs
VLAN 20 (Management VLAN)
Even though the ports on the Management VLAN link do not belong to any of the VLANs in the mesh, the link will be blocked if you enable Spanning Tree. This is because Spanning Tree operates per-switch and not per-VLAN.
VLAN 10
VLAN 30
VLAN 40
Switch 2
Switch 3

Figure 2-37. Example of Inadvertently Blocking a Management VLAN Link by Implementing Spanning Tree

Voice VLANs

Configuring voice VLANs separates voice traffic from data traffic and shields your voice traffic from broadcast storms. This section describes how to configure the switch for voice VLAN operation.

Operating Rules for Voice VLANs

- You must statically configure voice VLANs. GVRP and dynamic VLANs do not support voice VLAN operation.
- Configure all ports in a voice VLAN as tagged members of the VLAN. This ensures retention of the QoS (Quality of Service) priority included in voice VLAN traffic moving through your network.
- If a telephone connected to a voice VLAN includes a data port used for connecting other networked devices (such as PCs) to the network, then you must configure the port as a tagged member of the voice VLAN and a tagged or untagged member of the data VLAN you want the other networked device to use.

Components of Voice VLAN Operation

- **Voice VLAN(s):** Configure one or more voice VLANs on the switch. Some reasons for having multiple voice VLANs include:
  - Employing telephones with different VLAN requirements
  - Better control of bandwidth usage
  - Segregating telephone groups used for different, exclusive purposes

  Where multiple voice VLANs exist on the switch, you can use routing to communicate between telephones on different voice VLANs. .
- **Tagged/Untagged VLAN Membership:** If the appliances using a voice VLAN transmit tagged VLAN packets, then configure the member ports as tagged members of the VLAN. Otherwise, configure the ports as untagged members.

Voice VLAN Access Security

You can use port security configured on an individual port or group of ports in a voice VLAN. That is, you can allow or deny access to a phone having a particular MAC address. Refer to chapter titled “Configuring and Monitoring Port Security” in the *Access Security Guide* for your switch.

Note MAC authentication is not recommended in voice VLAN applications.

Effect of VLANs on Other Switch Features

Spanning Tree Operation with VLANs

Depending on the spanning-tree option configured on the switch, the spanning-tree feature may operate as a single instance across all ports on the switch (regardless of VLAN assignments) or multiple instance on a per-VLAN basis. For single-instance operation, this means that if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, regardless of whether the redundant links are in separate VLANs. In this case you can use port trunking to prevent Spanning Tree from unnecessarily blocking ports (and to improve overall network performance). For multiple-

instance operation, physically redundant links belonging to different VLANs can remain open. Refer to chapter 4, “Multiple Instance Spanning-Tree Operation” .

Note that Spanning Tree operates differently in different devices. For example, in the (obsolete, non-802.1Q) ProCurve Switch 2000 and the ProCurve Switch 800T, Spanning Tree operates on a per-VLAN basis, allowing redundant physical links as long as they are in separate VLANs.

IP Interfaces

There is a one-to-one relationship between a VLAN and an IP network interface. Since the VLAN is defined by a group of ports, the state (up/down) of those ports determines the state of the IP network interface associated with that VLAN. When a port-based VLAN or an IPv4 or IPv6 protocol-based VLAN comes up because one or more of its ports is up, the IP interface for that VLAN is also activated. Likewise, when a VLAN is deactivated because all of its ports are down, the corresponding IP interface is also deactivated.

VLAN MAC Address

The switches covered by this guide have one unique MAC address for all of their VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch. Likewise, you can assign an IP address to the VLAN interface, and when you Ping that address, ARP will resolve the IP address to this single MAC address. In a topology where a switch has multiple VLANs and must be connected to a device having a single forwarding database, such as the Switch 4000M, some cabling restrictions apply. For more on this topic, refer to “Multiple VLAN Considerations” on page 2-17.

Port Trunks

When assigning a port trunk to a VLAN, all ports in the trunk are automatically assigned to the same VLAN. You cannot split trunk members across multiple VLANs. Also, a port trunk is tagged, untagged, or excluded from a VLAN in the same way as for individual, untrunked ports.

Port Monitoring

If you designate a port on the switch for network monitoring, this port will appear in the Port VLAN Assignment screen and can be configured as a member of any VLAN. For information on how broadcast, multicast, and unicast packets are tagged inside and outside of the VLAN to which the

monitor port is assigned, refer to the section titled "VLAN-Related Problems" in the "Troubleshooting" appendix of the *Management and Configuration Guide* for your switch.

Jumbo Packet Support

Jumbo packet support is enabled per-VLAN and applies to all ports belonging to the VLAN. For more information, refer to the chapter titled "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

VLAN Restrictions

- A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN; VID = 1).
- A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged. (The "Untagged" designation enables VLAN operation with non 802.1Q-compliant devices.)
- A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.
- Prior to deleting a static VLAN, you must first re-assign all ports in the VLAN to another VLAN. You can use the **no vlan < *vid* >** command to delete a static VLAN. For more information, refer to "Creating a New Static VLAN (Port-Based or Protocol-Based) Changing the VLAN Context Level" on page 2-35.

GVRP

Contents

Overview 3-2

Introduction 3-3

General Operation 3-4

Per-Port Options for Handling GVRP "Unknown VLANs" 3-7

Per-Port Options for Dynamic VLAN Advertising and Joining 3-9

GVRP and VLAN Access Control 3-11

Advertisements and Dynamic Joins 3-11

Port-Leave From a Dynamic VLAN 3-11

Planning for GVRP Operation 3-12

Configuring GVRP On a Switch 3-13

Menu: Viewing and Configuring GVRP 3-13

CLI: Viewing and Configuring GVRP 3-14

Web: Viewing and Configuring GVRP 3-18

GVRP Operating Notes 3-18

Overview

This chapter describes GVRP and how to configure it with the switch's built-in interfaces, and assumes an understanding of VLANs, which are described in chapter 2, "Static Virtual LANs (VLANs)" .

For general information on how to use the switch's built-in interfaces, refer to these chapters in the *Management and Configuration Guide* for your switch:

- Chapter 3, "Using the Menu Interface"
- Chapter 4, "Using the Command Line Interface (CLI)"
- Chapter 5, "Using the Web Browser Interface
- Chapter 6, "Switch Memory and Configuration"

Introduction

Feature	Default	Menu	CLI	Web
view GVRP configuration	n/a	page 3-13	page 3-14	page 3-18
list static and dynamic VLANs on a GVRP-enabled switch	n/a	—	page 3-16	page 3-18
enable or disable GVRP	disabled	page 3-13	page 3-15	page 3-18
enable or disable GVRP on individual ports	enabled	page 3-13	page 3-15	—
control how individual ports handle advertisements for new VLANs	Learn	page 3-13	page 3-15	page 3-18
convert a dynamic VLAN to a static VLAN	n/a	—	page 3-17	—
configure static VLANs	DEFAULT_VLAN (VID = 1)	page 2-21	page 2-27	page 2-39

GVRP—GARP VLAN Registration Protocol—is an application of the Generic Attribute Registration Protocol—GARP. GVRP is defined in the IEEE 802.1Q standard, and GARP is defined in the IEEE 802.1D-1998 standard.

Note

To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (Refer to chapter 2, “Static Virtual LANs (VLANs)” .)

GVRP uses “GVRP Bridge Protocol Data Units” (“GVRP BPDUs”) to “advertise” static VLANs. In this manual, a GVRP BPDU is termed an *advertisement*. Advertisements are sent outbound from ports on a switch to the devices directly connected to those ports.

GVRP enables the switch to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across your network. After the switch creates a dynamic VLAN, you can optionally use the CLI **static <*vlan-id*>** command to

convert it to a static VLAN or allow it to continue as a dynamic VLAN for as long as needed. You can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.

Note: On the switches covered in this guide, GVRP can be enabled only if **max vlans** is set to no more than 256 VLANs.

General Operation

When GVRP is enabled on a switch, the VID for any static VLANs configured on the switch is *advertised* (using BPDUs—Bridge Protocol Data Units) out all ports, regardless of whether a port is up or assigned to any particular VLAN. A GVRP-aware port on another device that receives the advertisements over a link can dynamically join the advertised VLAN.

A dynamic VLAN (that is, a VLAN learned through GVRP) is tagged on the port on which it was learned. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch (internal source), but the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received through a link from another device (external source) on that specific port

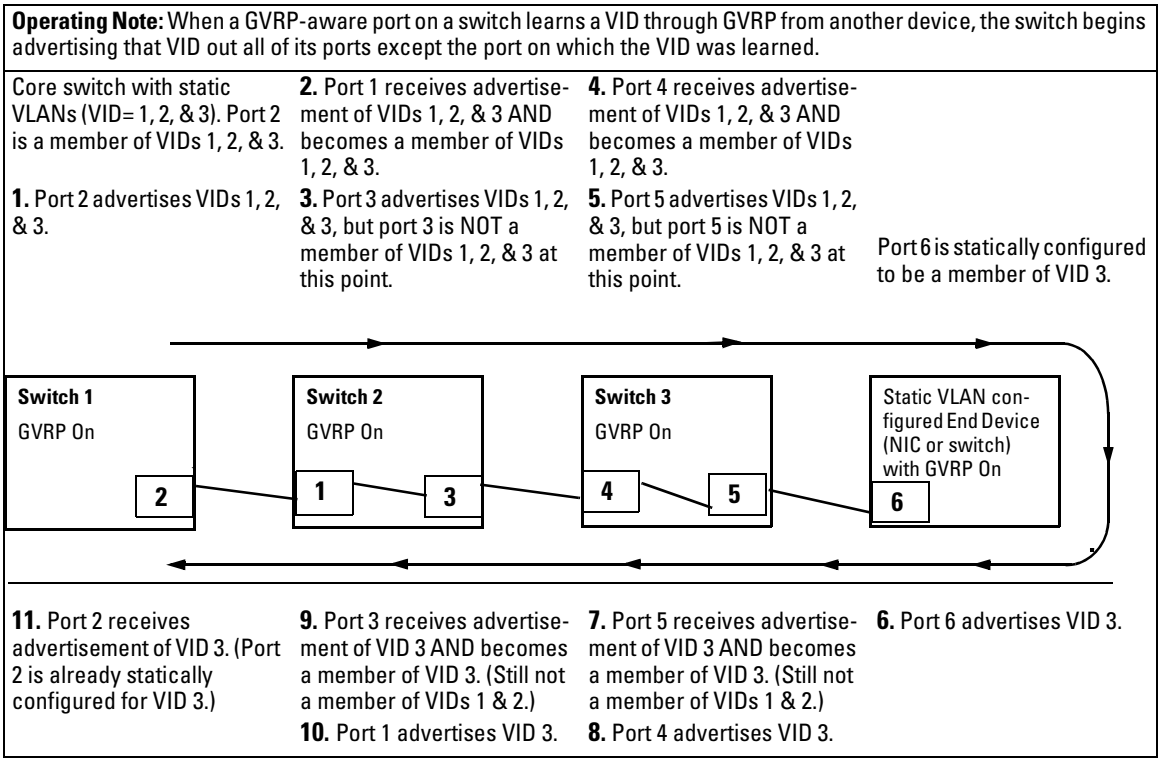

Operating Note: When a GVRP-aware port on a switch learns a VID through GVRP from another device, the switch begins advertising that VID out all of its ports except the port on which the VID was learned.
Core switch with static VLANs (VID= 1, 2, & 3). Port 2 is a member of VIDs 1, 2, & 3.
1. Port 2 advertises VIDs 1, 2, & 3.
2. Port 1 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.
3. Port 3 advertises VIDs 1, 2, & 3, but port 3 is NOT a member of VIDs 1, 2, & 3 at this point.
4. Port 4 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.
5. Port 5 advertises VIDs 1, 2, & 3, but port 5 is NOT a member of VIDs 1, 2, & 3 at this point.
Port 6 is statically configured to be a member of VID 3.
Switch 1
GVRP On
Switch 2
GVRP On
Switch 3
GVRP On
Static VLAN configured End Device (NIC or switch) with GVRP On
2
1
3
4
5
6
11. Port 2 receives advertisement of VID 3. (Port 2 is already statically configured for VID 3.)
9. Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)
10. Port 1 advertises VID 3.
7. Port 5 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)
8. Port 4 advertises VID 3.
6. Port 6 advertises VID 3.

Figure 3-1. Example of Forwarding Advertisements and Dynamic Joining

Note that if a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

For example, in the following figure, Tagged VLAN ports on switch “A” and switch “C” advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.

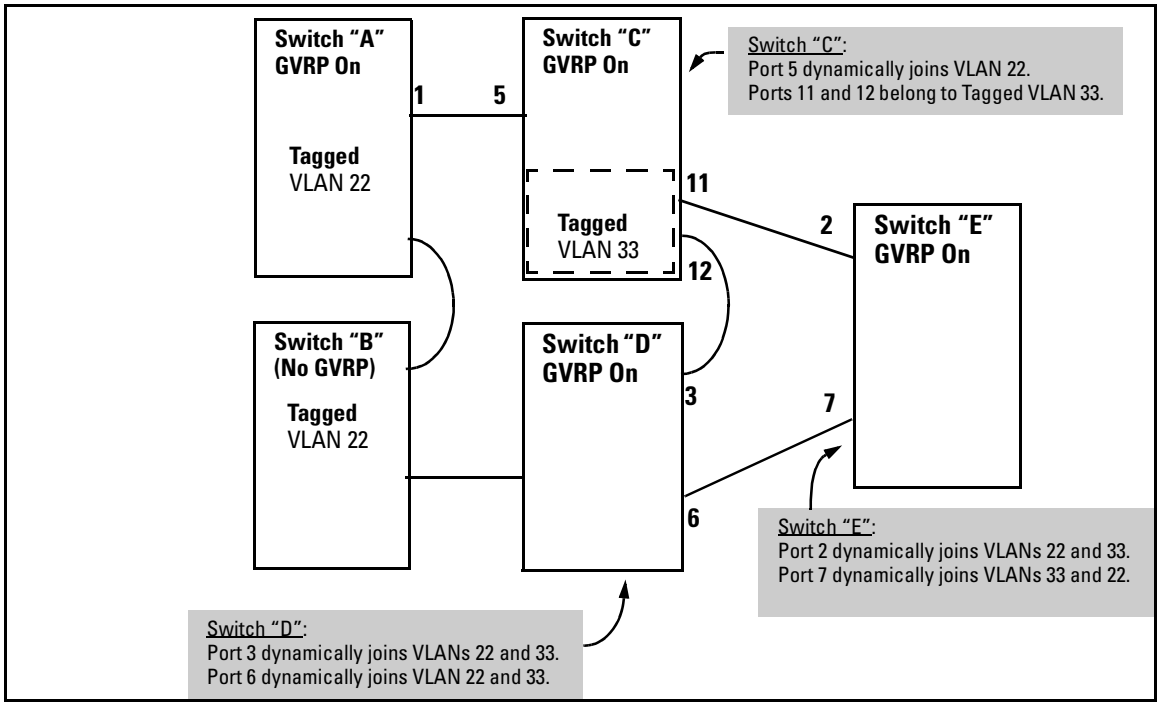


Figure 3-2. Example of GVRP Operation

Note

A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch "B", above). VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through.

A GVRP-aware port receiving advertisements has these options:

- If there is not already a static VLAN with the advertised VID on the receiving port, then dynamically create the VLAN and become a member.
- If the switch already has a static VLAN assignment with the same VID as in the advertisement, and the port is configured to **Auto** for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN's traffic. (For more detail on **Auto**, see "Per-Port Options for Dynamic VLAN Advertising and Joining" on page 3-9.)
- Ignore the advertisement for that VID.
- Don't participate in that VLAN.

Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:

- Send VLAN advertisements, and also receive advertisements for VLANs on other ports and dynamically join those VLANs.
- Send VLAN advertisements, but ignore advertisements received from other ports.
- Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices.

IP Addressing. A dynamic VLAN does not have an IP address, and moves traffic on the basis of port membership in VLANs. However, after GVRP creates a dynamic VLAN, you can convert it to a static VLAN. Note that it is then necessary to assign ports to the VLAN in the same way that you would for a static VLAN that you created manually. In the static state you can configure IP addressing on the VLAN and access it in the same way that you would any other static (manually created) VLAN.

Per-Port Options for Handling GVRP "Unknown VLANs"

An "unknown VLAN" is a VLAN that the switch learns of by receiving an advertisement for that VLAN on a port that is not already a member of that VLAN. If the port is configured to learn unknown VLANs, then the VLAN is dynamically created and the port becomes a tagged member of the VLAN. For example, suppose that in figure 3-2 (page 3-6), port 1 on switch "A" is connected to port 5 on switch "C". Because switch "A" has VLAN 22 statically configured, while switch "C" does not have this VLAN statically configured (and does not "Forbid" VLAN 22 on port 5), VLAN 22 is handled as an "Unknown VLAN" on port 5 in switch "C". Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch "A".

When you enable GVRP on a switch, you have the per-port join-request options listed in table 3-1:

Table 3-1. Options for Handling "Unknown VLAN" Advertisements:

Unknown VLAN Mode	Operation
Learn (the Default)	Enables the port to become a member of any unknown VLAN for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port on the same switch as a member.
Block	Prevents the port from joining any new dynamic VLANs for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port as a member.
Disable	Causes the port to ignore and drop all GVRP advertisements it receives and also prevents the port from sending any GVRP advertisements.

The CLI **show gvrp** command and the menu interface VLAN Support screen show a switch's current GVRP configuration, including the Unknown VLAN settings.

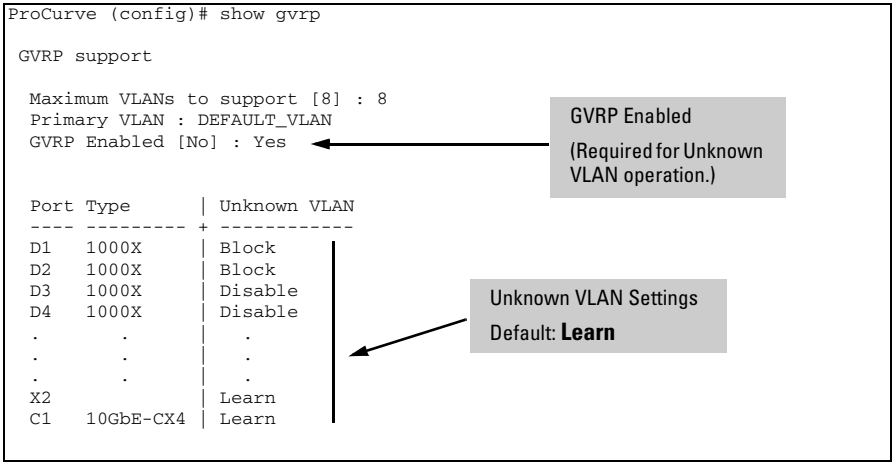


Figure 3-3. Example of GVRP Unknown VLAN Settings

Per-Port Options for Dynamic VLAN Advertising and Joining

Initiating Advertisements. As described in the preceding section, to enable dynamic joins, GVRP must be enabled and a port must be configured to Learn (the default). However, to send advertisements in your network, one or more static (**Tagged**, **Untagged**, or **Auto**) VLANs must be configured on one or more switches (with GVRP enabled), depending on your topology.

Enabling a Port for Dynamic Joins. You can configure a port to dynamically join a static VLAN. The join will then occur if that port subsequently receives an advertisement for the static VLAN. (This is done by using the **Auto** and **Learn** options described in table 3-2, on the next page.

Parameters for Controlling VLAN Propagation Behavior. You can configure an individual port to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP "Unknown VLAN" and the static VLAN configuration parameters, as described in the following table:

Table 3-2. Controlling VLAN Behavior on Ports with Static VLANs

Per-Port "Unknown VLAN" (GVRP) Configuration	Static VLAN Options—Per VLAN Specified on Each Port [1]		
	Port Activity: Tagged or Untagged (Per VLAN)[2]	**Port Activity: Auto[2] (Per VLAN)**	**Port Activity: Forbid (Per VLAN)[2]**
Learn (the Default)	The port: • Belongs to specified VLAN. • Advertises specified VLAN. • Can become a member of dynamic VLANs for which it receives advertisements. • Advertises dynamic VLANs that have at least one other port (on the same switch) as a member.	The port: • Will become a member of specified VLAN if it receives advertisements for specified VLAN from another device. • Will advertise specified VLAN. • Can become a member of other, dynamic VLANs for which it receives advertisements. • Will advertise a dynamic VLAN that has at least one other port (on the same switch) as a member.	The port: 1. Will not become a member of the specified VLAN. 2. Will not advertise specified VLAN. 3. Can become a member of other dynamic VLANs for which it receives advertisements. 4. Will advertise a dynamic VLAN that has at least one other port on the same switch as a member.
Block	The port: • Belongs to the specified VLAN. • Advertises this VLAN. • Will not become a member of new dynamic VLANs for which it receives advertisements. • Will advertise dynamic VLANs that have at least one other port as a member.	The port: • Will become a member of specified VLAN if it receives advertisements for this VLAN. • Will advertise this VLAN. • Will not become a member of new dynamic VLANs for which it receives advertisements. • Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.	The port: • Will not become a member of the specified VLAN. • Will not advertise this VLAN. • Will not become a member of dynamic VLANs for which it receives advertisements. • Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.
Disable	The port: • Is a member of the specified VLAN. • Will ignore GVRP PDUs. • Will not join any advertised VLANs. • Will not advertise VLANs.	The port: • Will not become a member of the specified VLAN. • Will ignore GVRP PDUs. • Will not join any dynamic VLANs. • Will not advertise VLANs.	The port: • Will not become a member of this VLAN. • Will ignore GVRP PDUs. • Will not join any dynamic VLANs. • Will not advertise VLANs.

[1] Each port of the switch must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for static VLAN(s) configured on the switch and also for dynamic VLANs the switch learns on other ports.

[2] To configure tagging, **Auto**, or **Forbid**, see "Configuring Static VLAN Per-Port Settings" on page 2-37 (for the CLI) or "Adding or Changing a VLAN Port Assignment" on page 2-25 (for the menu).

As the preceding table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

Note

In table 3-2, above, the Unknown VLAN parameters are configured on a per-port basis using the CLI. The Tagged, Untagged, Auto, and Forbid options are configured per static VLAN on every port, using either the menu interface or the CLI.

Because dynamic VLANs operate as Tagged VLANs, and because a tagged port on one device cannot communicate with an untagged port on another device, ProCurve recommends that you use Tagged VLANs for the static VLANs you will use to generate advertisements.

GVRP and VLAN Access Control

Advertisements and Dynamic Joins

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch's ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:

- Allow a port to advertise and/or join dynamic VLANs (Learn mode—the default).
- Allow a port to send VLAN advertisements, but not receive them from other devices; that is, the port cannot dynamically join a VLAN but other devices can dynamically join the VLANs it advertises (Block mode).
- Prevent a port from participating in GVRP operation (Disable mode).

Port-Leave From a Dynamic VLAN

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN (See "Converting a Dynamic VLAN to a Static VLAN" on page 3-17.)
- Reconfigure the port to **Block** or **Disable**

- Disable GVRP
- Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

Planning for GVRP Operation

These steps outline the procedure for setting up dynamic VLANs for a segment.

1. Determine the VLAN topology you want for each segment (broadcast domain) on your network.
2. Determine the VLANs that must be static and the VLANs that can be dynamically propagated.
3. Determine the device or devices on which you must manually create static VLANs in order to propagate VLANs throughout the segment.
4. Determine security boundaries and how the individual ports in the segment will handle dynamic VLAN advertisements. (See table 3-1 on page 3-8 and table 3-2 on page 3-10.)
5. Enable GVRP on all devices you want to use with dynamic VLANs and configure the appropriate "Unknown VLAN" parameter (**Learn**, **Block**, or **Disable**) for each port.
6. Configure the static VLANs on the switch(es) where they are needed, along with the per-VLAN parameters (**Tagged**, **Untagged**, **Auto**, and **Forbid**—see table 3-2 on page 3-10) on each port.
7. Dynamic VLANs will then appear automatically, according to the configuration options you have chosen.
8. Convert dynamic VLANs to static VLANs where you want dynamic VLANs to become permanent.

Configuring GVRP On a Switch

The procedures in this section describe how to:

- View the GVRP configuration on a switch
- Enable and disable GVRP on a switch
- Specify how individual ports will handle advertisements

To view or configure static VLANs for GVRP operation, refer to "Per-Port Static VLAN Configuration Options" on page 2-12.

Menu: Viewing and Configuring GVRP

1. From the Main Menu, select:

   2. Switch Configuration ...
   8. VLAN Menu ...
   1. VLAN Support

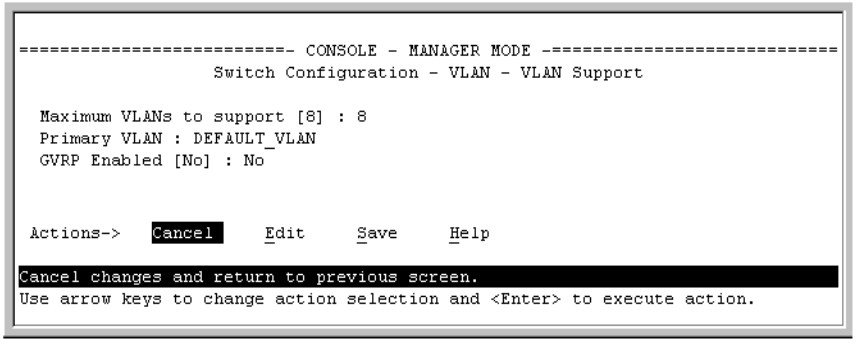

==========- CONSOLE - MANAGER MODE -==========
Switch Configuration - VLAN - VLAN Support
Maximum VLANs to support [8] : 8
Primary VLAN : DEFAULT_VLAN
GVRP Enabled [No] : No
Actions-> Cancel Edit Save Help
Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.

Figure 3-4. The VLAN Support Screen (Default Configuration)

2. Do the following to enable GVRP and display the Unknown VLAN fields:
   a. Press **[E]** (for **Edit**).
   b. Use ↓ to move the cursor to the **GVRP Enabled** field.
   c. Press the Space bar to select **Yes**.
   d. Press ↓ again to display the **Unknown VLAN** fields.

The Unknown VLAN fields enable you to configure each port to:
- Learn - Dynamically join any advertised VLAN and advertise all VLANs learned through other ports.
- Block - Do not dynamically join any VLAN, but still advertise all VLANs learned through other ports.
- Disable - Ignore and drop all incoming advertisements and do not transmit any advertisements.

```
============================-TELNET- MANAGER MODE -=============================
                    Switch Configuration - VLAN - VLAN Support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : Yes

  Port     Type       Unknown VLAN  Join   Leave  Leaveall
  ----  ---------  + ------------  -----  -----  --------
  D1    1000X      | Block         20     300    1000
  D2    1000X      | Block         20     300    1000
  D3    1000X      | Disable       20     300    1000
  D4    1000X      | Disable       20     300    1000
  D5    1000X      | Disable       20     300    1000
  D6    1000X      | Disable       20     300    1000
  D7    1000X      | Disable       20     300    1000
  D8    1000X      | Disable       20     300    1000

 Actions->   Cancel     Edit     Save     Help
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure 3-5. Example Showing Default Settings for Handling Advertisements

3. Use the arrow keys to select the port you want, and the Space bar to select Unknown VLAN option for any ports you want to change.
4. When you finish making configuration changes, press **[Enter]**, then **[S]** (for **Save**) to save your changes to the Startup-Config file.

CLI: Viewing and Configuring GVRP

GVRP Commands Used in This Section

show gvrp	below
gvrp	page 3-15
unknown-vlans	page 3-15

Displaying the Switch's Current GVRP Configuration. This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see chapter 2, "Static Virtual LANs (VLANs)" .)

Syntax: show gvrp *Shows the current settings.*

```
ProCurve (config)# show gvrp

 GVRP support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : No
```

Figure 3-6. Example of "Show GVRP" Listing with GVRP Disabled

```
ProCurve (config)# show gvrp

 GVRP support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : Yes


  Port Type       | Unknown VLAN
  ---- ---------- + ------------
  D1   1000X      | Block
  D2   1000X      | Block
  D3   1000X      | Disable
  D4   1000X      | Disable
  .       .       |   .
  .       .       |   .
  .       .       |   .
  X2              | Learn
  C1   10GbE-CX4  | Learn
```

This example includes non-default settings for the Unknown VLAN field for some ports.

Figure 3-7. Example of Show GVRP Listing with GVRP Enabled

Enabling and Disabling GVRP on the Switch. This command enables GVRP on the switch.

Syntax: gvrp

This example enables GVRP:

```
ProCurve(config)# gvrp
```

This example disables GVRP operation on the switch:

```
ProCurve(config)# no gvrp
```

Enabling and Disabling GVRP On Individual Ports. When GVRP is enabled on the switch, use the **unknown-vlans** command to change the Unknown VLAN field for one or more ports. You can use this command at either the Manager level or the interface context level for the desired port(s).

Syntax: interface < *port-list* > unknown-vlans < learn | block | disable >

Changes the Unknown VLAN field setting for the specified port(s).

For example, to change and view the configuration for ports A1-A2 to **Block**:

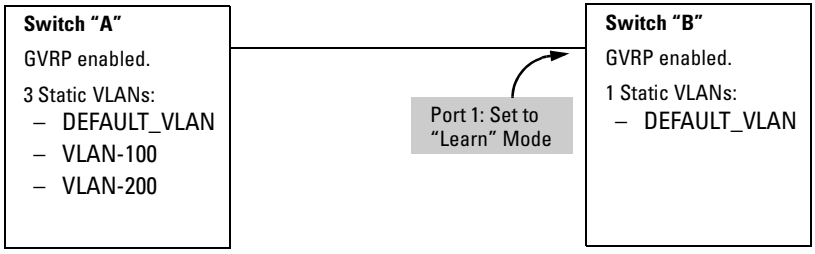
```
ProCurve (config)# interface d1-d2 unknown-vlans block
ProCurve (config)# show gvrp

 GVRP support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : Yes


  Port Type      | Unknown VLAN
  ---- --------- + ------------
  D1   1000X     | Block
  D2   1000X     | Block
  .       .      |   .
  .       .      |   .
  .       .      |   .
  X2             | Learn
  C1   10GbE-CX4 | Learn
```

Figure 3-8. Displaying the Static and Dynamic VLANs Active on the Switch

Syntax: show vlans

The **show vlans** *command lists all VLANs present in the switch.*

For example, in the following illustration, switch "B" has one static VLAN (the default VLAN), with GVRP enabled and port 1 configured to **Learn** for Unknown VLANs. Switch "A" has GVRP enabled and has three static VLANs: the default VLAN, VLAN-222, and VLAN-333. In this scenario, switch B will dynamically join VLAN-222 and VLAN-333:



The **show vlans** command lists the dynamic (and static) VLANs in switch "B" after it has learned and joined VLAN-100 and VLAN-200.

```
ProCurve (config)# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  VLAN ID Name                 | Status
  ------- -------------------- + ----------
  1       DEFAULT_VLAN         | Port-based
  100     GVRP_100             | Dynamic
  200     GVRP_200             | Dynamic
  300     GVRP_300             | Dynamic
  400     GVRP_400             | Dynamic
  500     GVRP_500             | Dynamic
  600     GVRP_600             | Dynamic
```

Dynamic VLANs Learned from Switch "A" through Port 1

Figure 3-9. Example of Listing Showing Dynamic VLANs

Converting a Dynamic VLAN to a Static VLAN. If a port on the switch has joined a dynamic VLAN, you can use the following command to convert that dynamic VLAN to a static VLAN:

Syntax: static < *dynamic-vlan-id* >

Converts the a dynamic VLAN to a static VLAN.

For example, to convert dynamic VLAN 333 (from the previous example) to a static VLAN:

```
ProCurve(config)# static 333
```

When you convert a dynamic VLAN to a static VLAN, all ports on the switch are assigned to the VLAN in Auto mode.

Web: Viewing and Configuring GVRP

To view, enable, disable, or reconfigure GVRP:

1. Click on the **Configuration** tab.
2. Click on **[VLAN Configuration]** and do the following:
   - To enable or disable GVRP, click on **GVRP Enabled**.
   - To change the Unknown VLAN field for any port:
     i. Click on **[GVRP Security]** and make the desired changes.
     ii. Click on **[Apply]** to save and implement your changes to the Unknown VLAN fields.

For web-based Help on how to use the web browser interface screen, click on the **[?]** button provided on the web browser screen.

GVRP Operating Notes

- A dynamic VLAN must be converted to a static VLAN before it can have an IP address.
- On the switches covered in this guide, GVRP can be enabled only if **max vlans** is set to no more than 256 VLANs.
- The total number of VLANs on the switch (static and dynamic combined) cannot exceed the current Maximum VLANs setting. For example, in the factory default state, the switch supports up to 256 VLANs. Any additional VLANs advertised to the switch will not be added unless you first increase the Maximum VLANs setting. In the Menu interface, click on **2. Switch Configuration ... | 8. VLAN Menu | 1. VLAN Support**. In the global config level of the CLI, use **max-vlans**.
- Converting a dynamic VLAN to a static VLAN and then executing the **write memory** command saves the VLAN in the startup-config file and makes it a permanent part of the switch's VLAN configuration.
- Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-ware will flood the GVRP (multicast) advertisement packets out all ports.
- GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, you must first convert it to a static VLAN.

- Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.
- By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices, as well as the dynamic VLANs the switch has learned.
- A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.
- A VLAN enabled for jumbo traffic cannot be used to create a dynamic VLAN. A port belonging to a statically configured, jumbo-enabled VLAN cannot join a dynamic VLAN.

4

Multiple Instance Spanning-Tree Operation

Contents

Overview 4-3

802.1s Multiple Spanning Tree Protocol (MSTP) 4-6

MSTP Structure 4-7

How MSTP Operates 4-9

MST Regions 4-9

Regions, Legacy STP and RSTP Switches, and the Common Spanning Tree (CST) 4-11

MSTP Operation with 802.1Q VLANs 4-12

Terminology 4-13

Operating Rules 4-15

MSTP Compatibility with RSTP or STP 4-16

Configuring MSTP 4-17

Planning an MSTP Application 4-17

MSTP Configuration Overview 4-19

Configuring MSTP Operation Mode and Global Settings 4-21

Configuring MSTP Per-Port Parameters 4-26

Configuring Per Port Parameters 4-26

Configuring BPDU Filtering 4-30

Configuring BPDU Protection 4-31

Configuring MST Instance Parameters 4-35

Configuring MST Instance Per-Port Parameters 4-37

Enabling or Disabling Spanning Tree Operation 4-40

Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another 4-40

MSTP VLAN Configuration Enhancement 4-42

PreConfiguring VLANs in an MST Instance 4-43

Configuring MSTP Instances with the VLAN Range Option 4-44

Operating Notes for the VLAN Configuration Enhancement . . . 4-46

How to Save Your Current Configuration 4-47
Displaying MSTP Statistics and Configuration 4-49
Displaying Global MSTP Status 4-50
Displaying Detailed Port Information 4-52
Displaying Status for a Specific MST Instance 4-53
Displaying the MSTP Configuration 4-54
Troubleshooting an MSTP Configuration 4-58
Displaying the Change History of Root Bridges 4-58
Displaying Debug Counters for All MST Instances 4-61
Displaying Debug Counters for One MST Instance 4-62
Displaying Debug Counters for Ports in an MST Instance 4-64
Field Descriptions in MSTP Debug Command Output 4-66
Troubleshooting MSTP Operation 4-69
Loop Protection 4-70
Configuring Loop Protection 4-71
Viewing Loop Protection Status 4-72

Overview

The switches covered in this guide, use the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard.

MSTP Features

802.1s Spanning Tree Protocol	Default Setting	Page Ref
Viewing MSTP Status and Configuration	n/a	page 4-49
Configuring MSTP Operation Mode and Global Parameters	Disabled	page 4-21 and following
Configuring Basic Port Connectivity Parameters	admin-edge-port: No-disabled auto-edge-port: Yes-enabled bpdu-filter: No-disabled bpdu-protection: No-disabled hello-time: 2 path-cost: auto point-to-point MAC: Force-True priority: 128 (multiplier: 8) root-guard: No-disabled tcn-guard: No-disabled loop protection: Send disable	page 4-26 and following
Configuring MSTP Instance Parameters	instance (MSTPI): none priority: 32768 (multiplier: 8)	page 4-35
Configuring MSTP Instance Per-Port Parameters	path-cost: auto priority: 128 (multiplier: 8)	page 4-37
Enabling/Disabling MSTP Spanning Tree Operation	Disabled	page 4-40
Enabling an Entire MST Region at Once	n/a	page 4-40

Without spanning tree, having more than one active path between a pair of nodes causes loops in the network, which can result in duplication of messages, leading to a "broadcast storm" that can bring down the network.

Note

MSTP cannot protect against loops when there is an unmanaged device on the network that drops spanning tree packets, or may fail to detect loops where this is an edge port configured with client authentication (802.1X, Web and MAC authentication). To protect against the formation of loops in these cases, you can use the loop protection feature (see "Loop Protection" on page 4-70).

Multiple-Instance spanning tree operation (802.1s) ensures that only one active path exists between any two nodes in a spanning-tree *instance*. A spanning-tree instance comprises a unique set of VLANs, and belongs to a specific spanning-tree *region*. A region can comprise multiple spanning-tree instances (each with a different set of VLANs), and allows one active path among regions in a network. Applying VLAN tagging to the ports in a multiple-instance spanning-tree network enables blocking of redundant links in one instance while allowing forwarding over the same links for non-redundant use by another instance.

For example, suppose you have three switches in a region configured with VLANs grouped into two instances, as follows:

VLANs	Instance 1	Instance 2
10, 11, 12	Yes	No
20, 21, 22	No	Yes

The logical and physical topologies resulting from these VLAN/Instance groupings result in blocking on different links for different VLANs:

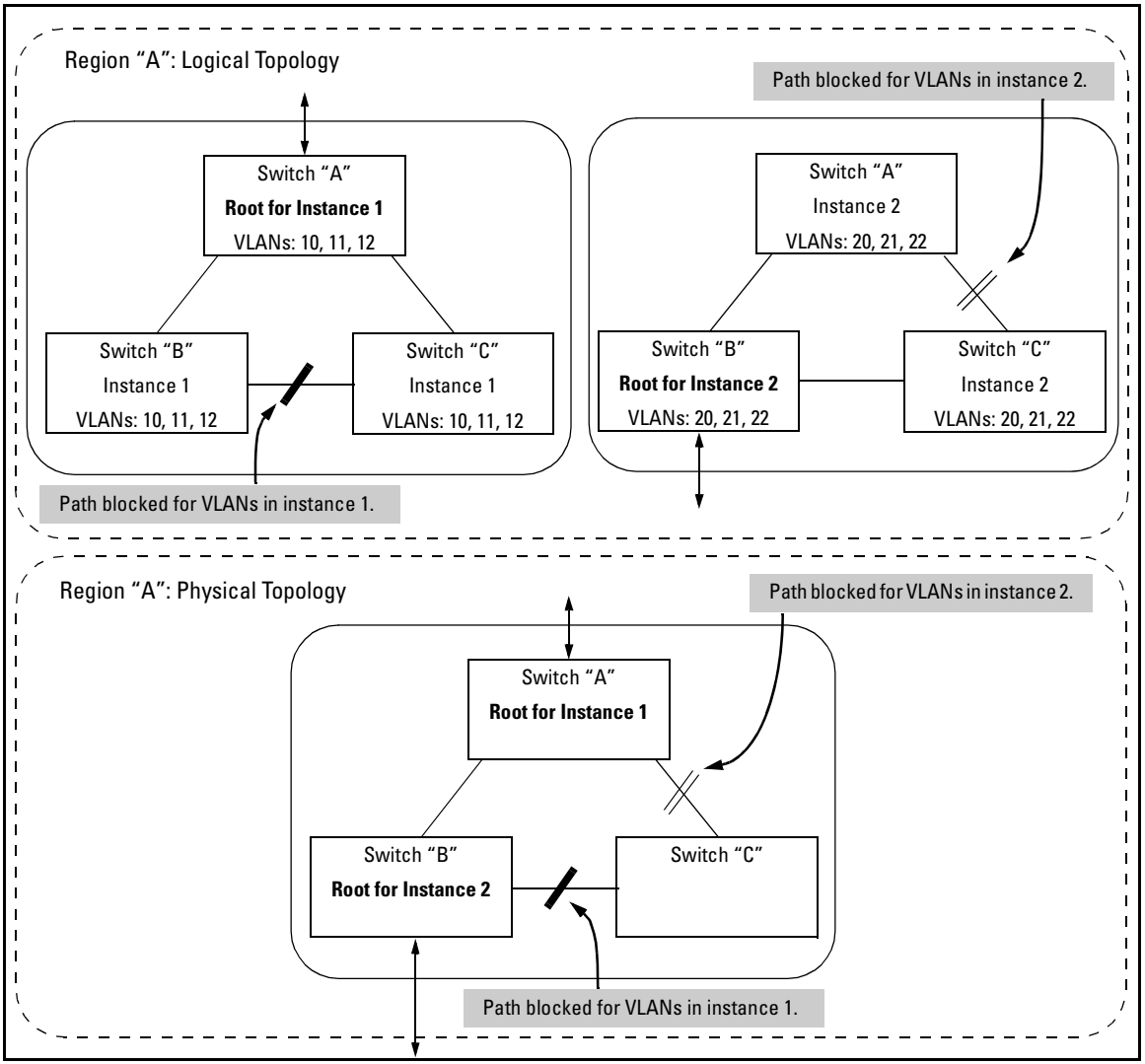


Figure 4-1. Example of a Multiple Spanning-Tree Application

802.1s Multiple Spanning Tree Protocol (MSTP)

The 802.1D and 802.1w spanning tree protocols operate without regard to a network's VLAN configuration, and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology. The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

While the per-VLAN spanning tree approach adopted by some vendors overcomes the network utilization problems inherent in using STP or RSTP, using a per-VLAN technology with multiple VLANs can overload the switch's CPU. MSTP on the switches covered in this guide complies with the IEEE 802.1s standard, and extends STP and RSTP functionality to map multiple independent spanning tree instances onto a physical topology. With MSTP, each spanning tree instance can include one or more VLANs and applies a separate, per-instance forwarding topology. Thus, where a port belongs to multiple VLANs, it may be dynamically blocked in one spanning tree instance, but forwarding in another instance. This achieves load-balancing across the network while keeping the switch's CPU load at a moderate level (by aggregating multiple VLANs in a single spanning tree instance). MSTP provides fault tolerance through rapid, automatic reconfiguration if there is a failure in a network's physical topology.

With MSTP-capable switches, you can create a number of MST regions containing multiple spanning tree instances. This requires the configuration of a number of MSTP-capable switches. However, it is NOT necessary to do this. You can just enable MSTP on an MSTP-capable switch and a spanning tree instance is created automatically. This instance always exists by default when spanning tree is enabled, and is the spanning tree instance that communicates with STP and RSTP environments. The MSTP configuration commands operate exactly like RSTP commands and MSTP is backward-compatible with the RSTP-enabled and STP-enabled switches in your network.

Caution

Spanning tree interprets a switch mesh as a single link. Because the switch automatically gives faster links a higher priority, the default MSTP parameter settings are usually adequate for spanning tree operation. Also, because incorrect MSTP settings can adversely affect network performance, you should not change the MSTP settings from their default values unless you have a strong understanding of how spanning tree operates.

In a mesh environment, the default MSTP timer settings (**Hello Time** and **Forward Delay**) are usually adequate for MSTP operation. Because a packet crossing a mesh may traverse several links within the mesh, using smaller-than-default settings for the MSTP **Hello Time** and **Forward Delay** timers can cause unnecessary topology changes and end-node connectivity problems.

For MSTP information beyond what is provided in this manual, refer to the IEEE 802.1s standard.

MSTP Structure

MSTP maps active, separate paths through separate spanning tree instances and between MST regions. Each MST region comprises one or more MSTP switches. Note that MSTP recognizes an STP or RSTP LAN as a distinct spanning-tree region.

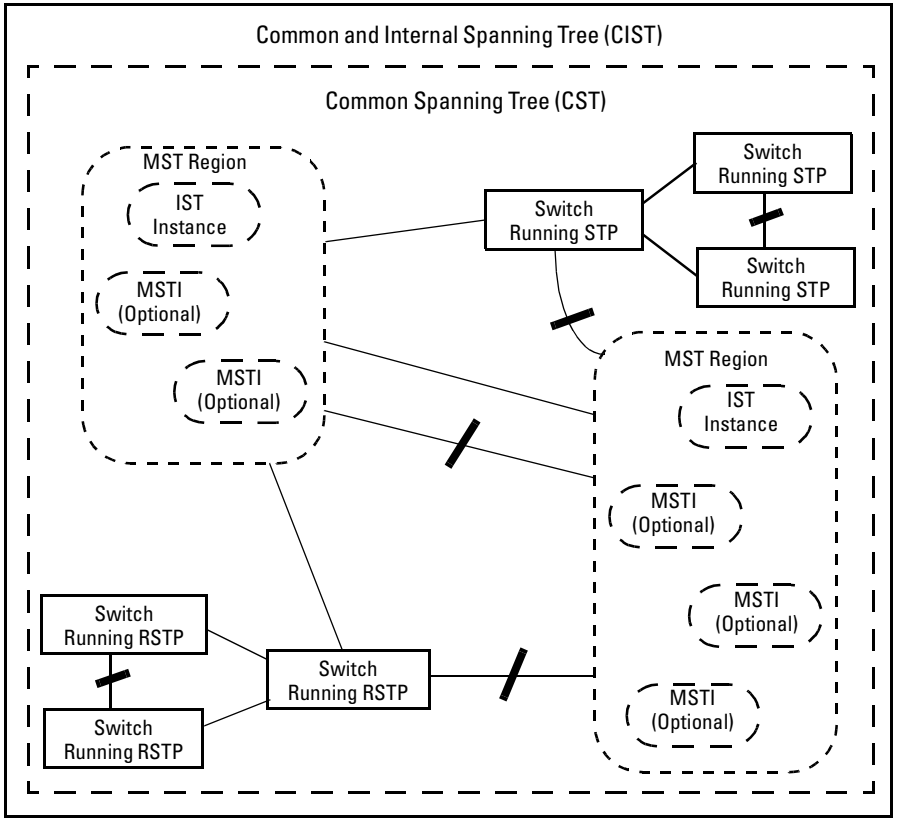


Figure 4-2. Example of MSTP Network with Legacy STP and RSTP Devices Connected

Common and Internal Spanning Tree (CIST): The CIST identifies the regions in a network and administers the CIST root bridge for the network, the root bridge for each region, and the root bridge for each spanning-tree instance in each region.

Common Spanning Tree (CST): The CST administers the connectivity among the MST regions, STP LANs, and RSTP LANs in a bridged network.

MST Region: An MST region comprises the VLANs configured on physically connected MSTP switches. All switches in a given region must be configured with the same VLANs, the same Multiple Spanning Tree Instances (MSTIs), and the same MST configuration identifiers.

Internal Spanning Tree (IST): The IST administers the topology within a given MST region. When you configure a switch for MSTP operation, the switch automatically includes all of the static VLANs configured on the switch in a single, active spanning tree topology (instance) within the IST. This is termed the "IST instance". Any VLANs you subsequently configure on the switch are added to this IST instance. To create separate forwarding paths within a region, group specific VLANs into different Multiple Spanning Tree Instances (MSTIs). (Refer to "Multiple Spanning Tree Instance (MSTI)", below.)

Types of Multiple Spanning Tree Instances: A multiple spanning tree network comprises separate spanning-tree instances existing in an MST region. (There can be multiple regions in a network.) Each instance defines a single forwarding topology for an exclusive set of VLANs. By contrast, an STP or RSTP network has only one spanning tree instance for the entire network, and includes all VLANs in the network. (An STP or RSTP network operates as a single-instance network.) A region can include two types of STP instances:

- **Internal Spanning-Tree Instance (IST Instance):** This is the default spanning tree instance in any MST region. It provides the root switch for the region and comprises all VLANs configured on the switches in the region that are not specifically assigned to Multiple Spanning Tree Instances (MSTIs, described below).

  Within a region, the IST instance provides a loop-free forwarding path for all VLANs associated with it. VLANs that are not associated with an MSTI are, by default, associated with the IST instance. Note that the switch automatically places dynamic VLANs (resulting from GVRP operation) in the IST instance. Dynamic VLANs cannot exist in an MSTI (described below).

- **Multiple Spanning Tree Instance (MSTI):** This type of configurable spanning tree instance comprises all static VLANs you specifically assign to it, and must include at least one VLAN. The VLAN(s) you assign to an

MSTI must initially exist in the IST instance of the same MST region. When you assign a static VLAN to an MSTI, the switch removes the VLAN from the IST instance. (Thus, you can assign a VLAN to only one MSTI in a given region.) All VLANs in an MSTI operate as part of the same single spanning tree topology. (The switch does not allow dynamic VLANs in an MSTI.)

Caution

When you enable MSTP on the switch, the default MSTP spanning tree configuration settings comply with the values recommended in the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Note that inappropriate changes to these settings can result in severely degraded network performance. For this reason, *ProCurve strongly recommends that changing these default settings be reserved only for experienced network administrators who have a strong understanding of the IEEE 802.1D/w/s standards and operation.*

How MSTP Operates

In the factory default configuration, spanning tree operation is on. Also, the switch retains its currently configured spanning tree parameter settings when disabled. Thus, if you disable spanning tree, then later re-enable it, the parameter settings will be the same as before spanning tree was disabled. The switch also includes a "Pending" feature that enables you to exchange MSTP configurations with a single command. (Refer to "Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another" on page 4-40.)

Note

The switch automatically senses port identity and type, and automatically defines spanning-tree parameters for each type, as well as parameters that apply across the switch. Although these parameters can be adjusted, *ProCurve strongly recommends leaving these settings in their default configurations unless the proposed changes have been supplied by an experienced network administrator who has a strong understanding of the IEEE 802.1D/w/s standards and operation.*

MST Regions

All MSTP switches in a given region must be configured with the same VLANs. Also, each MSTP switch within the same region must have the same VLAN-to-instance assignments. (A VLAN can belong to only one instance within any region.) Within a region:

- All of the VLANs belonging to a given instance compose a single, active spanning-tree topology for that instance.
- Each instance operates independently of other regions.

Between regions there is a single, active spanning-tree topology.

How Separate Instances Affect MSTP Operation. Assigning different groups of VLANs to different instances ensures that those VLAN groups use independent forwarding paths. For example, in figure 4-3 each instance has a different forwarding path.

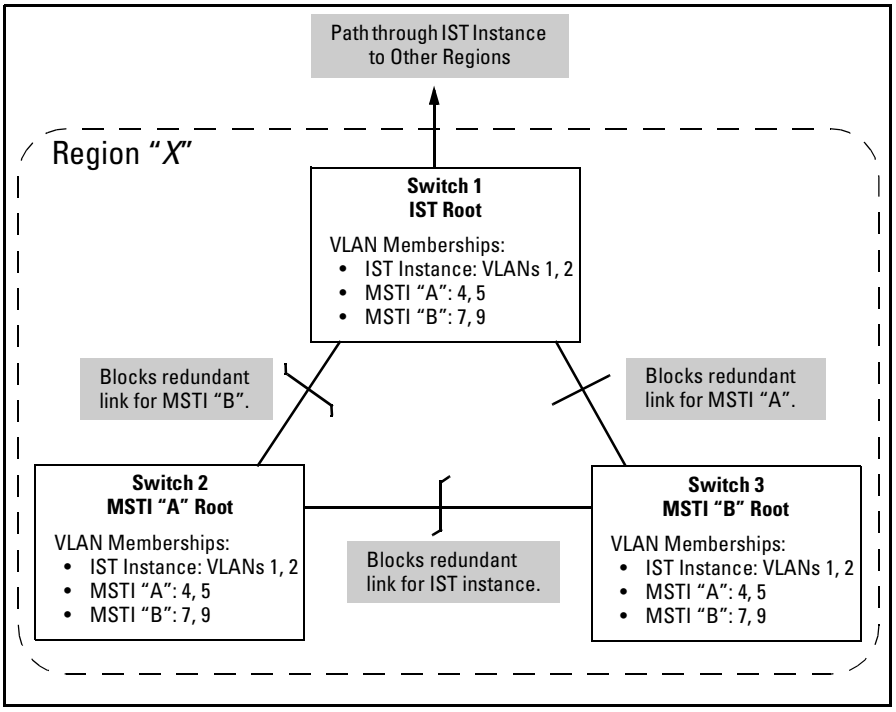

Path through IST Instance to Other Regions
Region "X"
Switch 1
IST Root
VLAN Memberships:
• IST Instance: VLANs 1, 2
• MSTI "A": 4, 5
• MSTI "B": 7, 9
Blocks redundant link for MSTI "B".
Blocks redundant link for MSTI "A".
Switch 2
MSTI "A" Root
VLAN Memberships:
• IST Instance: VLANs 1, 2
• MSTI "A": 4, 5
• MSTI "B": 7, 9
Blocks redundant link for IST instance.
Switch 3
MSTI "B" Root
VLAN Memberships:
• IST Instance: VLANs 1, 2
• MSTI "A": 4, 5
• MSTI "B": 7, 9

Figure 4-3. Active Topologies Built by Three Independent MST Instances

While allowing only one active path through a given instance, MSTP retains any redundant physical paths in the instance to serve as backups (blocked) paths in case the existing active path fails. Thus, if an active path in an instance fails, MSTP automatically activates (unblocks) an available backup to serve as the new active path through the instance for as long as the original active path is down. Note also that a given port may simultaneously operate in different states (forwarding or blocking) for different spanning-tree instances within the same region. This depends on the VLAN memberships to which the port is assigned. For example, if a port belongs to VLAN 1 in the IST instance of a region and also belongs to VLAN 4 in MSTI "*x*" in the same region, the port may apply different states to traffic for these two different instances.

Within a region, traffic routed between VLANs in separate instances can take only one physical path. To ensure that traffic in all VLANs within a region can travel between regions, all of the boundary ports for each region should belong to all VLANs configured in the region. Otherwise, traffic from some areas within a region could be blocked from moving to other regions.

All MSTP switches (as well as STP and RSTP switches) in a network use BPDUs (Bridge Protocol Data Units) to exchange information from which to build multiple, active topologies in the individual instances within a region and between regions. From this information:

- The MSTP switches in each LAN segment determine a designated bridge and designated port or trunk for the segment.
- The MSTP switches belonging to a particular instance determine the root bridge and root port or trunk for the instance.
- For the IST instance within a region, the MSTP switches linking that region to other regions (or to STP or RSTP switches) determine the IST root bridge and IST root port or trunk for the region. (For any Multiple Spanning-Tree instance—MSTI—in a region, the regional root may be a different switch that is not necessarily connected to another region.)
- The MSTP switches block redundant links within each LAN segment, across all instances, and between regions, to prevent any traffic loops.

As a result, each individual instance (spanning tree) within a region determines its regional root bridge, designated bridges, and designated ports or trunks.

Regions, Legacy STP and RSTP Switches, and the Common Spanning Tree (CST)

The IST instance and any MST instances in a region exist only within that region. Where a link crosses a boundary between regions (or between a region and a legacy STP or RSTP switch), traffic is forwarded or blocked as determined by the Common Spanning Tree (CST). The CST ensures that there is only one active path between any two regions, or between a region and a switch running STP and RSTP. (Refer to figure 4-2 on page 4-7.)

MSTP Operation with 802.1Q VLANs

As indicated in the preceding sections, within a given MST instance, a single spanning tree is configured for all VLANs included in that instance. This means that if redundant physical links exist in separate VLANs within the same instance, MSTP blocks all but one of those links. However, you can prevent the bandwidth loss caused by blocked redundant links for different VLANs in an instance by using a port trunk. The following example shows how you can use a port trunk with 802.1Q (tagged) VLANs and MSTP without unnecessarily blocking any links or losing any bandwidth.

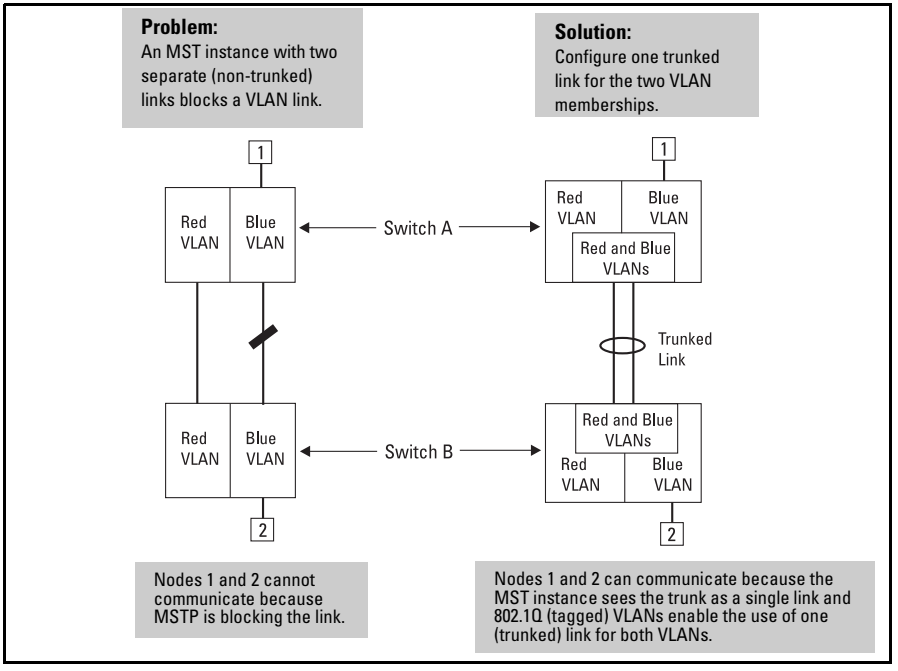

Problem:
An MST instance with two separate (non-trunked) links blocks a VLAN link.
Solution:
Configure one trunked link for the two VLAN memberships.
1
Red VLAN
Blue VLAN
Switch A
Red VLAN
Blue VLAN
Red and Blue VLANs
Trunked Link
Red VLAN
Blue VLAN
Switch B
Red and Blue VLANs
Red VLAN
Blue VLAN
2
Nodes 1 and 2 cannot communicate because MSTP is blocking the link.
Nodes 1 and 2 can communicate because the MST instance sees the trunk as a single link and 802.1Q (tagged) VLANs enable the use of one (trunked) link for both VLANs.

Figure 4-4. Example of Using a Trunked Link To Support Multiple VLAN Connectivity within the Same MST Instance

Note

All switches in a region should be configured with the VLANs used in that region, and all ports linking MSTP switches together should be members of all VLANs in the region. Otherwise, the path to the root for a given VLAN will be broken if MSTP selects a spanning tree through a link that does not include that VLAN.

Terminology

BPDU — Acronym for bridge protocol data unit. BPDUs are data messages that are exchanged between the switches within an extended LAN that use a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by placing redundant switch ports in a backup, or blocked, state.

BPDU Filtering — Spanning-tree configuration mode that prevents the switch from receiving and transmitting BPDU frames on a specific port (see page 4-30 for details).

BPDU Protection — Spanning-tree configuration mode which disables a port where BPDU frames are received (see page 4-31 for details).

Bridge: See "MSTP Bridge".

Common and Internal Spanning Tree (CIST): Comprises all LANs, STP, and RSTP bridges and MSTP regions in a network. The CIST automatically determines the MST regions in a network and defines the root bridge (switch) and designated port for each region. The CIST includes the Common Spanning Tree (CST), the Internal Spanning Tree (IST) within each region, and any multiple spanning-tree instances (MSTIs) in a region.

Common Spanning Tree (CST): Refers to the single forwarding path the switch calculates for STP (802.1D) and RSTP (802.1w) topologies, and for inter-regional paths in MSTP (802.1s) topologies. Note that all three types of spanning tree can interoperate in the same network. Also, the MSTP switch interprets a device running 802.1D STP or 802.1w RSTP as a separate region. (Refer to figure 4-2 on page 4-7.)

Internal Spanning Tree (IST): Comprises all VLANs within a region that are not assigned to a multiple spanning-tree instance configured within the region. All MST switches in a region should belong to the IST. In a given region "X", the IST root switch is the regional root switch and provides information on region "X" to other regions.

MSTP (Multiple Spanning Tree Protocol): A network supporting MSTP allows multiple spanning tree instances within configured regions, and a single spanning tree among regions, STP bridges, and RSTP bridges.

MSTP BPDU (MSTP Bridge Protocol Data Unit): These BPDUs carry region-specific information, such as the region identifier (region name and revision number). If a switch receives an MSTP BPDU with a region identifier that differs from its own, then the port on which that BPDU was received is on the boundary of the region in which the switch resides.

MSTP Bridge: In this manual, an MSTP bridge is a switch (or another 802.1s-compatible device) configured for MSTP operation.

MST Region: An MST region forms a multiple spanning tree domain and is a component of a single spanning-tree domain within a network. For switches internal to the MST region:

- All switches have identical MST configuration identifiers (region name and revision number).
- All switches have identical VLAN assignments to the region's IST and (optional) MST instances.
- One switch functions as the designated bridge (IST root) for the region.
- No switch has a point-to-point connection to a bridging device that cannot process RSTP BPDUs.

RSTP — Rapid Spanning Tree Protocol, defined in IEEE 802.1w and ratified in IEEE 802.1D-2004.

Spanning-tree — Generic term to refer to the many spanning-tree flavors: now deprecated STP, RSTP and VLAN-aware MSTP.

STP — Spanning Tree Protocol, part of the original IEEE 802.1D specification. The 2004 edition completely deprecates STP. Both RSTP and MSTP have fallback modes to handle STP.

SNMP — Simple Network Management Protocol, used to remotely manage network devices.

Operating Rules

- All switches in a region must be configured with the same set of VLANs, as well as the same MST configuration name and MST configuration number.
- Within a region, a VLAN can be allocated to either a single MSTI or to the region's IST instance.
- All switches in a region must have the same VID-to-MST instance assignment.
- There is one root MST switch per configured MST instance.
- Because boundary ports provide the VLAN connectivity between regions, all boundary ports on a region's root switch should be configured as members of all static VLANs defined in the region.
- There is one root switch for the Common and Internal Spanning Tree (CIST). At any given time, all switches in the network will use the per-port **hello-time** parameter assignments configured on the CIST root switch.
- Where multiple MST regions exist in a network, there is only one active, physical communication path between any two regions, or between an MST region and an STP or RSTP switch. MSTP blocks any other physical paths as long as the currently active path remains in service.
- Within a network, an MST region appears as a virtual RSTP bridge to other spanning tree entities (other MST regions, and any switches running 802.1D or 802.1w spanning-tree protocols).
- Within an MSTI, there is one physical communication path between any two nodes, regardless of how many VLANs belong to the MSTI. Within an IST instance, there is also one spanning tree across all VLANs belonging to the IST instance.
- An MSTI comprises a unique set of VLANs and forms a single spanning-tree instance within the region to which it belongs.
- A dynamic VLAN learned by GVRP will always be placed in the IST instance and cannot be moved to any configured MST instance.

  Starting in software release 13.*x*.*x*, dynamically learned GVRP VLANs can be mapped to MSTIs and support MSTP load balancing.
- You can preconfigure static and dynamic VLAN ID-to-MSTI mappings before the VLAN is created on the switch. Later, when the static VLAN ID is configured or a dynamic GVRP VLAN is learned, the VLAN is automatically associated with the preconfigured MSTI. For more information, refer to the **spanning-tree instance vlan** command description on page 4-36.
- Communication between MST regions uses a single spanning tree.

- If a port on a switch configured for MSTP receives a legacy (STP/802.1D or RSTP/802.1w) BPDU, it automatically operates as a legacy port. In this case, the MSTP switch interoperates with the connected STP or RSTP switch as a separate MST region.
- Within an MST region, there is one logical forwarding topology per instance, and each instance comprises a unique set of VLANs. Where multiple paths exist between a pair of nodes using VLANs belonging to the same instance, all but one of those paths will be blocked for that instance. However, if there are different paths in different instances, all such paths are available for traffic. Separate forwarding paths exist through separate spanning tree instances.
- A port can have different states (forwarding or blocking) for different instances (which represent different forwarding paths).
- MSTP interprets a switch mesh as a single link.

MSTP Compatibility with RSTP or STP

IEEE 802.1s MSTP includes RSTP functionality and is designed to be compatible with both IEEE 802.1D and 802.1w spanning-tree protocols. Using the default configuration values, your switches will interoperate effectively with RSTP and STP devices. MSTP automatically detects when the switch ports are connected to non-MSTP devices in the spanning tree and communicates with those devices using 802.1D or 802.1w STP BPDU packets, as appropriate.

To enable effective interoperation with STP (802.1D) configured devices, however, you may need to adjust the default configuration values. Here are two such examples:

- The rapid state transitions employed by MSTP may result in an increase in the rates of frame duplication and misordering in the switched LAN. To allow the switch to support applications and protocols that may be sensitive to frame duplication and misordering, you can disable rapid transitions by setting the Force Protocol Version parameter to **STP-compatible**. The value of this parameter applies to all ports on the switch. See information on **force version** on page 4-22.
- One of the benefits of MSTP is the implementation of a larger range of port path costs, which accommodates higher network speeds. However, this can create some incompatibility between devices running the older 802.1D STP. You can adjust to this incompatibility by implementing the global **spanning-tree legacy-path cost** command (see page 4-23). See also the “Note on Path Cost” below.

Note on Path Cost

RSTP and MSTP implement a greater range of path costs than 802.1D STP, and use different default path cost values to account for higher network speeds. These values are shown below.

Port Type	802.1D STP Path Cost	RSTP and MSTP Path Cost
10 Mbps	100	2 000 000
100 Mbps	10	200 000
1 Gbps	5	20 000

Because the maximum value for the path cost allowed by 802.1D STP is 65535, devices running that version of spanning tree cannot be configured to match the values defined by MSTP, at least for 10 Mbps and 100 Mbps ports. In LANs where there is a mix of devices running 802.1D STP, RSTP, and/or MSTP, you should reconfigure the devices so the path costs match for ports with the same network speeds.

Configuring MSTP

This section outlines the main pre-requisites for configuring MSTP in your network, and describes MSTP settings at the global level, per individual port, and per MST instance.

Planning an MSTP Application

Before configuring MSTP, keep in mind the following tips and considerations:

- Ensure that the VLAN configuration in your network supports all of the forwarding paths necessary for the desired connectivity. All ports connecting one switch to another within a region and one switch to another between regions should be configured as members of all VLANs configured in the region.
- Configure all ports or trunks connecting one switch to another within a region as members of all VLANs in the region. Otherwise, some VLANs could be blocked from access to the spanning-tree root for an instance or for the region.

- Plan individual regions based on VLAN groupings. That is, plan on all MSTP switches in a given region supporting the same set of VLANs. Within each region, determine the VLAN membership for each spanning-tree instance. (Each instance represents a single forwarding path for all VLANs in that instance.)
- Verify that there is one logical spanning-tree path through the following:
  - Any inter-regional links
  - Any IST or MST instance within a region
  - Any legacy (802.1D or 802.1w) switch or group of switches. (Where multiple paths exist between an MST region and a legacy switch, expect the CST to block all but one such path.)
- Determine the root bridge and root port for each instance.
- Determine the designated bridge and designated port for each LAN segment.
- Determine which VLANs to assign to each instance, and use port trunks with 802.1Q VLAN tagging where separate links for separate VLANs would result in a blocked link preventing communication between nodes on the same VLAN. (Refer to "MSTP Operation with 802.1Q VLANs" on page 4-12.)
- Identify the edge ports connected to end nodes and enable the admin-edge-port setting for these ports. Leave the admin-edge-port setting disabled for ports connected to another switch, a bridge, or a hub.

Note on MSTP Rapid State Transitions

Under some circumstances the rapid state transitions employed by MSTP can increase the rates of frame duplication and misordering in the switched LAN. To allow MSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version (**force-version**) parameter to **stp-compatible** allows MSTP to operate with rapid transitions disabled. The value of this parameter applies to all ports on the switch. See the information on **force-version** on page 4-22.

MSTP Configuration Overview

This section describes the general steps for configuring MSTP via the CLI, assuming that you have already determined the VLANs you want MSTP to use (see "Planning an MSTP Application" on page 4-17). A description of each MSTP command syntax is provided in the following sections.

1. **Configure MSTP global parameters**.

   This step involves configuring the following:

   - Required parameters for MST region identity:

     Region Name: **spanning-tree config-name**

     Region Revision Number: **spanning-tree config-revision**

   - Optional MSTP parameter changes for region settings:

     ProCurve recommends that you leave these parameters at their default settings for most networks. See the "Caution" on page 4-9.

     – The maximum number of hops before the MSTP BPDU is discarded: **spanning-tree max-hops** (default: 20)

     – Force-Version operation: **spanning-tree force-version**

     – Forward Delay: **spanning-tree forward-delay**

     – Hello Time (if it is the root device): **spanning-tree hello-time**

     – Maximum age to allow for STP packets before discarding: **spanning-tree maximum-age**

     – Device spanning-tree priority. Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority. **spanning-tree priority**

2. **Configure per port parameters.**

   ProCurve recommends that you use the default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. Other features you might consider include BPDU Filtering or BPDU Protection—these provide additional per-port control over spanning-tree operations and security on the switch.

3. **Configure MST instances.**
   - Configure one instance for each VLAN group that you want to operate as an active topology within the region to which the switch belongs. When you create the instance, you must include a minimum of one VID. You can add more VIDs later if desired.

     spanning-tree instance < *n* > **vlan** < *vid* >

     To move a VLAN from one instance to another, first use **no spanning-tree instance** < *n* > **vlan** < *vid* > to unmap the VLAN from the current instance, then add the VLAN to the other instance. (While the VLAN is unmapped from an MSTI, it is associated with the region's IST instance.)

4. **Configure the priority for each instance.**
   spanning-tree instance < *n* > priority < *n* >

5. **Configure MST instance port parameters.**

   ProCurve recommends that you apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. For example, you might want to set the path cost value for the port(s) used by a specific MST instance.
   spanning-tree instance < *1..16* >< *port-list* > **path-cost** < *auto* | *1..200000000* >

   Alternatively, leaving this setting at the default (auto) allows the switch to calculate the path-cost from the link speed.

6. **Enable spanning-tree operation on the switch**.
   spanning-tree

For an example of a complete MSTP network configuration:

- Go to the ProCurve Web site at **www.procurve.com/support**.
- Click on **Configuration examples**.
- Click on **ProCurve Switch 8212zl** (the 6120 switches work like the 8212zl in this regard).
- Under **STP Example**, click on **ProCurve & Cisco Spanning Tree Interoperability**.

Configuring MSTP Operation Mode and Global Settings

The commands in this section apply at the switch (global) level. For details of how to configure spanning tree settings on individual ports, see "Configuring MSTP Per-Port Parameters" on page 4-26.

MSTP Global Command	Page
spanning-tree	*
config-name < *ascii-string* >	4-21
config-revision < *revision-number* >	4-22
force-version < stp-compatible | rstp-operation | mstp-operation>	4-22
forward-delay	4-23
hello-time < 1..10 >	4-23
legacy-mode	4-23
legacy-path-cost	4-23
max-hops < *hop-count* >	4-23
maximum-age	4-23
pending	4-24
priority	4-25
trap errant-bpdu	4-25

** Enabling MSTP operation using the **spanning-tree** global command is the final step in the configuration process. See "Enabling or Disabling Spanning Tree Operation" on page 4-40.*

Syntax: [no] spanning-tree config-name < *ascii-string* >

This command resets the configuration name of the MST region in which the switch resides. This name can include up to 32 nonblank characters and is case-sensitive. On all switches within a given MST region, the configuration names must be identical. Thus, if you want more than one MSTP switch in the same MST region, you must configure the identical region name on all such switches. If you retain the default configuration name on a switch, it cannot exist in the same MST region with another switch.
(Default Name: A text string using the hexadecimal representation of the switch's MAC address)

The **no** *form of the command overwrites the currently configured name with the default name.*

Note: *This option is available only when the switch is configured for MSTP operation. Also, there is no defined limit on the number of regions you can configure.*

Syntax: spanning-tree config-revision < *revision-number* >

This command configures the revision number you designate for the MST region in which you want the switch to reside. This setting must be the same for all switches residing in the same region. Use this setting to differentiate between region configurations in situations such as the following:

- *Changing configuration settings within a region where you want to track the configuration versions you use*
- *Creating a new region from a subset of switches in a current region and want to maintain the same region name.*
- *Using the* **pending** *option to maintain two different configuration options for the same physical region.*

Note that this setting must be the same for all MSTP switches in the same MST region. (Range: **0 - 65535***; Default:* **0***)*

Note: *This option is available only when the switch is configured for MSTP operation.*

Syntax: spanning-tree force-version < stp-compatible | rstp-operation | mstp-operation >

Sets the spanning-tree compatibility mode. This command forces the switch to emulate behavior of earlier versions of spanning tree protocol, or return to MSTP behavior. The command is useful in test or debug applications, and removes the need to reconfigure the switch for temporary changes in spanning-tree operation.

stp-compatible: *The switch applies 802.1D STP operation on all ports.*

rstp-operation: *The switch applies 802.1w operation on all ports except those ports where it detects a system using 802.1D Spanning Tree.*

mstp-operation: *The switch applies 802.1s MSTP operation on all ports where compatibility with 802.1D or 802.1w spanning tree protocols is not required.*

Note that even when mstp-operation is selected, if the switch detects an 802.1D BPDU or an 802.1w BPDU on a port, it communicates with the device linked to that port using STP or RSTP BPDU packets. Also, if errors are encountered as described in the "Note on MSTP Rapid State Transitions" on page 4-18, setting **force-version** *to* **stp-compatible** *forces the MSTP switch to communicate out all ports using operations that are compatible with IEEE 802.1D STP.*

Syntax: spanning-tree forward-delay

Sets time the switch waits between transitioning from listening to learning and from learning to forwarding states.

(*Range: 4 - 30; Default:* **15**.)

Syntax: spanning-tree legacy-mode

Sets spanning-tree protocol to operate in 802.1D legacy mode (STP-compatible).

(*Default:* **MSTP-operation**.)

The **no** *form of the command returns the switch to the default 802.1s native mode (MSTP-operation).*

Syntax: spanning-tree legacy-path-cost

Sets spanning-tree to operate with 802.1d (legacy) path cost values.

(*Default:* **802.1t**.)

The **no** *form of the command returns the switch to the default 802.1t (not legacy) path cost values.*

Syntax: spanning-tree hello-time < 1..10 >

If MSTP is running and the switch is operating as the CIST root for your network, this command specifies the time in seconds between transmissions of BPDUs for all ports on the switch configured with the **Global** *option. (the default). This parameter applies in MSTP, RSTP and STP modes. During MSTP operation, you can override this global setting on a per-port basis with this command:* **spanning-tree < *port-list* > hello-time < 1..10 >** (see page 4-27). (*Default:* **2**.)

Syntax: spanning-tree max-hops < *hop-count* >

This command resets the number of hops allowed for BPDUs in an MST region. When an MSTP switch receives a BPDU, it decrements the hop-count setting the BPDU carries. If the hop-count reaches zero, the receiving switch drops the BPDU. Note that the switch does not change the message-age and maximum-age data carried in the BPDU as it moves through the MST region and is propagated to other regions. (Range: 1 - 40; Default: 20)

Syntax: spanning-tree maximum age

Sets the maximum age of received STP information before it is discarded.

(*Default:* **20**.)

Syntax: spanning-tree pending < apply | config-name | config-revision | instance | reset >

Manipulates the pending MSTP configuration. The command is useful in test or debug applications, and enables rapid reconfiguration of the switch for changes in spanning-tree operation.

apply: *Apply pending MSTP configuration (swaps active and pending configurations).*

config-name: *Sets the pending MST region configuration name (default is switch's MAC address).*

config-revision: *Sets the pending MST region configuration revision number (default is 0).*

instance: *Change pending MST instance configuration.*

reset: *Copy active configuration to pending.*

Syntax: spanning-tree priority < priority-multiplier >

Every switch running an instance of MSTP has a Bridge Identifier, which is a unique identifier that helps distinguish this switch from all others. The switch with the lowest Bridge Identifier is elected as the root for the tree.

The Bridge Identifier is composed of a configurable Priority component (2 bytes) and the bridge's MAC address (6 bytes). The ability to change the Priority component provides flexibility in determining which switch will be the root for the tree, regardless of its MAC address.

This command sets the switch (bridge) priority for the designated region in which the switch resides. The switch compares this priority with the priorities of other switches in the same region to determine the root switch for the region. The lower the priority value, the higher the priority. (If there is only one switch in the region, then that switch is the root switch for the region.) The root bridge in a region provides the path to connected regions for the traffic in VLANs assigned to the region's IST instance. (Traffic in VLANs assigned to a numbered STP instance in a given region moves to other regions through the root switch for that instance.)

The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. That is, when you specify a priority multiplier value of 0 - 15, the actual priority assigned to the switch is:

(*priority-multiplier*) x 4096

*For example, if you configure "***2***" as the priority-multiplier on a given MSTP switch, then the* **Switch Priority** *setting is 8,192.*

Note: *If multiple switches in the same MST region have the same priority setting, then the switch with the lowest MAC address becomes the root switch for that region.*

Syntax: spanning-tree trap errant-bpdu

Enables SNMP traps for errant-BPDUs. Note that this command is designed to be used in conjunction with the spanning-tree bpdu-filter command (see page 4-30) and bpdu-protection command (see page 4-31).

The **no** *form of the command disables traps on the switch.*

(*Default:* **Disabled**.)

Configuring MSTP Per-Port Parameters

In an MSTP topology, you configure per-port parameters in the global configuration context.

In most cases, ProCurve recommends that you use the default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links. Some port parameters (such as **admin-edge-port**) affect all MSTI instances that consist of VLANs configured on the port; other port parameters (such as **path-cost**) affect only the specified MST.

Per Port Command	Page
spanning-tree < *port-list* >	
admin-edge-port	below
auto-edge-port	4-27
bpdu-filter	4-30
bpdu-protection	4-32
hello-time < global | 1..10 >	4-27
mcheck	4-27
path-cost < auto | 200000000 >	4-36
point-to-point-mac < force-true | force-false | auto>	4-25
priority <priority-multiplier>	4-25
root-guard	4-29
tcn-guard	4-30

Configuring Per Port Parameters

Syntax: [no] spanning-tree <port-list> admin-edge-port

Enable **admin-edge-port** *on ports connected to end nodes. During spanning tree establishment, ports with* **admin-edge-port** *enabled transition immediately to the forwarding state. If a bridge or switch is detected on the segment, the port automatically operates as non-edge, not enabled. (Default:* **No** *- disabled)*

If **admin-edge-port** *is disabled on a port and* **auto-edge-port** *has not been disabled, the* **auto-edge-port** *setting controls the behavior of the port.*

The **no spanning-tree < *port-list* > admin-edge-port** *command disables edge-port operation on the specified ports.*

Syntax: [no] spanning-tree < *port-list* > auto-edge-port

Supports the automatic identification of edge ports. The port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets. If **admin-edge-port** *is enabled for a port, the setting for* **auto-edge-port** *is ignored whether set to yes or no. If* **admin-edge-port** *is set to* **No**, *and* **auto-edge-port** *has not been disabled (set to* **No***), then the* **auto-edge-port** *setting controls the behavior of the port. (Default:* **Yes - enabled***)*

The **no spanning-tree < *port-list* > auto-edge-port** *command disables* **auto-edge-port** *operation on the specified ports.*

Syntax: spanning-tree < *port-list* > hello-time < global | 1 - 10 >

When the switch is the CIST root, this parameter specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports. This interval also applies to all ports in all switches downstream from each port in the < *port-list*>*. A setting of* **global** *indicates that the ports in* < *port-list*> *on the CIST root are using the value set by the global spanning-tree* **hello-time** *value (page 4-23). When a given switch "X" is not the CIST root, the per-port* **hello-time** *for all active ports on switch "X" is propagated from the CIST root, and is the same as the* **hello-time** *in use on the CIST root port in the currently active path from switch "X" to the CIST root. (That is, when switch "X" is not the CIST root, then the upstream CIST root's port* **hello-time** *setting overrides the* **hello-time** *setting configured on switch "X").*

(Default Per-Port setting: **Use Global***.*
Default Global Hello-Time: **2***.)*

Syntax: spanning-tree < *port-list* > mcheck

Forces a port to send RST/MST BPDUs for 3 seconds. This tests whether all STP bridges on the attached LAN have been removed and the port can migrate to native MSTP mode and use RST/MST BPDUs for transmission.

Syntax: spanning-tree < *port-list* > path-cost < auto | 1..200000000 >

Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree. In the default configuration (auto) the switch determines a port's path cost by the port's type:

- *10 Mbps:* **2000000**
- *100 Mbps:* **200000**
- *1 Gbps:* **20000**

Refer to "Note on Path Cost" on page 4-17 for information on compatibility with devices running 802.1D STP for the path cost values

(Default: Auto).

Syntax: spanning-tree < *port-list* > point-to-point-mac < true | false | auto >

This parameter informs the switch of the type of device to which a specific port connects.

true ***(default)****: Indicates a point-to-point link to a device such as a switch, bridge, or end-node.*

false*: Indicates a connection to a hub (which is a shared LAN segment).*

auto: *Causes the switch to set Force-False on the port if it is not running at full duplex. (Connections to hubs are half-duplex.)*

Syntax: spanning-tree < *port-list* > priority < priority-multiplier >

MSTP uses this parameter to determine the port(s) to use for forwarding. The port with the lowest priority number has the highest priority for use. The range is 0 to 240, and is configured by specifying a multiplier from 0 - 15. When you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

(*priority-multiplier*) *x* 16

*For example, if you configure "***2***" as the priority multiplier on a given port, then the actual* **Priority** *setting is 32. Thus, after you specify the port priority multiplier, the switch displays the actual port priority (and not the multiplier) in the* **show spanning-tree** *or* **show spanning-tree < *port-list* >** *displays.*

You can view the actual multiplier setting for ports by executing **show running** *and looking for an entry in this format:*

spanning-tree < *port-list* > priority < *priority-multiplier* >

For example, configuring port A2 with a priority multiplier of "3" results in this line in the **show running** *output:*

```
spanning-tree A2 priority 3
```

Syntax: spanning-tree < *port-list* > root-guard

MSTP only. When a port is enabled as **root-guard**, *it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior STP BPDUs. (A superior BPDU contains "better" information on the root bridge and/or path cost to the root bridge, which would normally replace the current root bridge selection.)*

The superior BPDUs received on a port enabled as **root-guard** *are ignored. All other BPDUs are accepted and the external devices may belong to the spanning tree as long as they do not claim to be the Root device.*

Use this command on MSTP switch ports that are connected to devices located in other administrative network domains to:

- *Ensure the stability of the core MSTP network topology so that undesired or damaging influences external to the network do not enter.*
- *Protect the configuration of the CIST root bridge that serves as the common root for the entire network.*

Default: Disabled.

Syntax: spanning-tree < *port-list* > tcn-guard

When **tcn-guard** *is enabled for a port, it causes the port to stop propagating received topology change notifications and topology changes to other ports.*
(Default: **No** *- disabled)*

Configuring BPDU Filtering

The STP BPDU filter feature allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets and stay locked in the spanning-tree forwarding state. All other ports will maintain their role.

Here are some sample scenarios in which this feature may be used:

- To have STP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.
- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of spanning-tree operations.
- To protect the network from denial of service attacks that use spoofing BPDUs by dropping incoming BPDU frames. For this scenario, BPDU protection offers a more secure alternative, implementing port shut down and a detection alert when errant BPDU frames are received (see page 4-32 for details).

Caution

Ports configured with the BPDU filter mode remain active (learning and forward frames); however, spanning-tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and disable the bpdu-filter (using the **no** command).

Command Syntax and Example. The following command is used to configure BPDU filters.

Syntax: [no] spanning-tree <port-list | all> bpdu-filter

Enables/disables the BPDU filter feature on the specified port(s). The bpdu-filter option forces a port to ***always*** *stay in the forwarding state and be excluded from standard STP operation.*

For example, to configure BPDU filtering on port a9, enter:

```
ProCurve(config)# spanning-tree a9 bpdu-filter
```

Viewing BPDU Filtering. The **spanning-tree show** < port> **configuration** command displays the BPDU's filter state.

```
ProCurve(config)# show spanning-tree a9 config

  ...
                  | Path      Prio  Admin Auto  Admin Hello  Root   TCN     BPDU
  Port  Type      | Cost      rity  Edge  Edge  PtP   Time   Guard  Guard   Flt
  ----- --------- + --------- ----- ----- ----- ----- ------ ------ ------ ----
  A9    100/1000T | Auto      128   No    Yes   True  Global No     No     Yes
```

Column showing BPDU filter status

Figure 4-5. Example of BPDU Filter in Show Spanning Tree Configuration Command

BPDU filters per port are displayed as separate entries of the spanning tree category within the configuration file.

```
ProCurve(config)# show configuration
  . . .
  spanning-tree
  spanning-tree A9 bpdu-filter
  spanning-tree C7 bpdu-filter
  spanning-tree Trk2 priority 4
  . . .
```

Rows showing ports with BPDU filters enabled

Figure 4-6. Example of BPDU Filters in the Show Configuration Command

Configuring BPDU Protection

BPDU protection is a security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection would be applied to edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, the feature will disable that port and alert the network manager via an SNMP trap as shown in Figure 4-7.

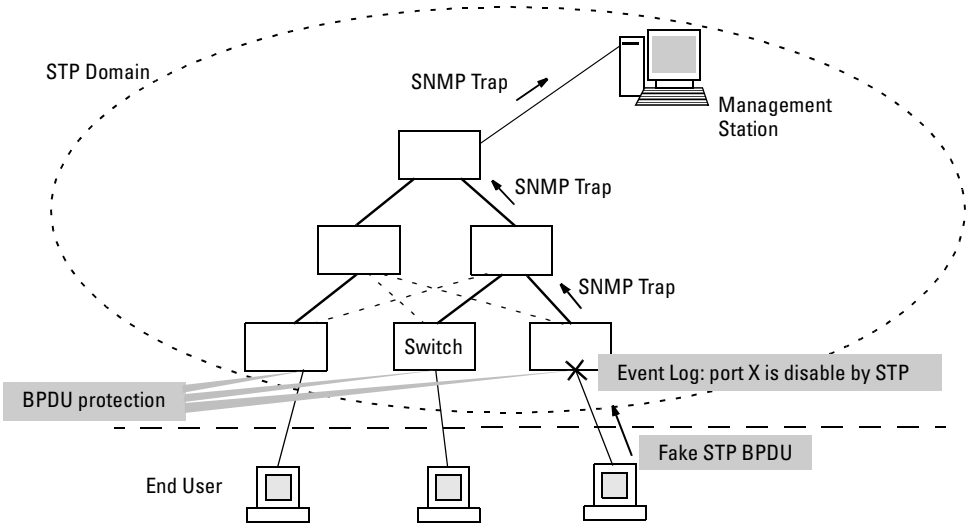


Figure 4-7. Example of BPDU Protection Enabled at the Network Edge

The following commands allow you to configure BPDU protection.

Syntax: [no] spanning-tree <*port-list*> bpdu-protection

Enables/disables the BPDU protection feature on a port

Syntax: [no] spanning-tree <*port-list*> bpdu-protection-timeout <*timeout*>

Configures the duration of time when protected ports receiving unauthorized BPDUs will remain disabled. The default value of 0 (zero) sets an infinite timeout (that is, ports that are disabled by **bpdu-protection** *are not, by default, re-enabled automatically). (Range: 0-65535 seconds; Default: 0)*

Syntax: [no] spanning-tree trap errant-bpdu

Enables/disables the sending of errant BPDU traps.

Caution This command should only be used to guard edge ports that are not expected to participate in STP operations. Once BPDU protection is enabled, it will disable the port as soon as any BPDU packet is received on that interface.

Example. To configure BPDU protection on ports 1 to 10 with SNMP traps enabled, enter:

```
ProCurve(config)# spanning-tree 1-10 bpdu protection
ProCurve(config)# spanning-tree trap errant-bpdu
```

The following steps will then be set in process:

1. When an STP BPDU packet is received on ports 1-10, STP treats it as an unauthorized transmission attempt and shuts down the port that the BPDU came in on.
2. An event message is logged and an SNMP notification trap is generated.
3. The port remains disabled until re-enabled manually by a network administrator using the **interface** <*port-list*> **enable** command.

Note

To re-enable the bpdu-protected ports automatically, configure a timeout period using the **spanning-tree bpdu-protection-timeout** command.

Viewing BPDU Protection Status. The **show spanning-tree bpdu-protection** command displays a summary listing of ports with BPDU protection enabled. To display detailed per port status information, enter the specific port number(s) as shown in Figure 4-8 below.

```
ProCurve(config)# show spanning-tree bpdu-protection a1

 Status and Counters - STP BPDU Protection Information

  BPDU Protection Timeout (sec) : 0
  Protected Ports : A1

  Port Type         Protection    State          Errant BPDUs
  ---- ------------ ------------- -------------- ---------------
  A1   100/1000T    Yes           Bpdu Error     1
```

Specifying the port displays additional status information for the designated ports.

Figure 4-8. Example of Show Spanning Tree BPDU Protection Command

BPDU protected ports are displayed as separate entries of the spanning tree category within the configuration file.

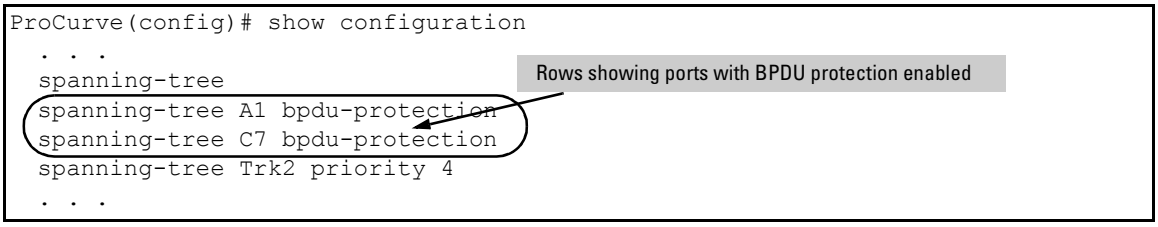


Figure 4-9. Example of BPDU Filters in the Show Configuration Command

Configuring MST Instance Parameters

When you enable MSTP on the switch, a spanning tree instance is enabled automatically. The switch supports up to sixteen configurable MST instances for each VLAN group that you want to operate as an active topology within the region to which the switch belongs. When creating an instance, you must include a minimum of one VID. You can add more VIDs later if desired.

Command	Page
[no] spanning-tree instance < 1..16 > vlan < *vid*> [*vid..vid*] no spanning-tree instance < 1..16 >	4-27
spanning-tree instance < 1..16 > priority < 0..15 >	4-35

Syntax: [no] spanning-tree instance < 1..16 > vlan < *vid* [*vid..vid*] >
no spanning-tree instance < 1..16 >

Configuring MSTP on the switch automatically configures the IST instance and places all statically and dynamically configured VLANs on the switch into the IST instance. This command creates a new MST instance (MSTI) and moves the VLANs you specify from the IST to the MSTI.

You must map at least one VLAN to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region.

The **no** *form of the command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the* **no** *form of the command deletes the specified MSTI.*

When you remove a VLAN from an MSTI, the VLAN returns to the IST instance, where it can remain or be re-assigned to another MSTI configured in the region.

Note: *Starting in software release 13.x.x, you can enter the* ***spanning-tree instance vlan*** *command before a static or dynamic VLAN is configured on the switch to preconfigure VLAN ID-to-MSTI mappings. No error message is displayed. Later, each newly configured VLAN that has already been associated with an MSTI is automatically assigned to the MSTI.*

This new default behavior differs from automatically including configured (static and dynamic) VLANs in the IST instance and requiring you to manually assign individual static VLANs to an MSTI.

Syntax: [no] spanning-tree instance < 1..16 > vlan < *vid* [*vid..vid*] >
no spanning-tree instance < 1..16 >
— Continued —

Note: *The valid VLAN IDs that you can map to a specified MSTI are from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement allows you to preconfigure MSTP topologies before the VLAN IDs associated with each instance exist on a switch.*

When you use preconfigured VLAN ID-to-MSTI topologies, ensure that MSTP switches remain in the same region by mapping all VLAN IDs used in the region to the same MSTIs on each regional switch.

When you upgrade switch software to release 13.x.x and later, the existing MSTP topology configuration is automatically saved. All existing VLAN ID-to-MSTI assignments are maintained on a switch for uninterrupted MSTP network operation.

Syntax: spanning-tree instance < 1..16 > priority < priority-multiplier >

This command sets the switch (bridge) priority for the designated instance. This priority is compared with the priorities of other switches in the same instance to determine the root switch for the instance. The lower the priority value, the higher the priority. (If there is only one switch in the instance, then that switch is the root switch for the instance.) The IST regional root bridge provides the path to instances in other regions that share one or more of the same VLAN(s).

The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. That is, when you specify a priority multiplier value of 0 - 15, the actual priority assigned to the switch for the specified MST instance is:

(*priority-multiplier*) x 4096

*For example, if you configure "***5***" as the priority-multiplier for MST Instance 1 on a given MSTP switch, then the* **Switch Priority** *setting is 20,480 for that instance in that switch.*

Note: *If multiple switches in the same MST instance have the same priority setting, then the switch with the lowest MAC address becomes the root switch for that instance.*

Configuring MST Instance Per-Port Parameters

Command	Page
spanning-tree instance < 1..16 > < port-list > path-cost < auto | 1..200000000 >	4-37
spanning-tree instance < 1..16 > < *port-list* > priority < *priority-multiplier* >	4-38
spanning-tree < *port-list* > priority < *priority-multiplier* >	4-39

Syntax: spanning-tree instance < 1..16 > < *port-list* > path-cost < auto | 1..200000000 >

This command assigns an individual port cost for the specified MST instance. (For a given port, the path cost setting can be different for different MST instances to which the port may belong.) The switch uses the path cost to determine which ports are the forwarding ports in the instance; that is which links to use for the active topology of the instance and which ports to block. The settings are either **auto** *or in a range from 1 to 200,000,000. With the* **auto** *setting, the switch calculates the path cost from the link speed:*

10 Mbps — 2000000

100 Mbps — 200000

1 Gbps — 20000

(Default: **Auto***)*

Syntax: spanning-tree instance < 1..16 >< *port-list* > priority <*priority-multiplier*>

This command sets the priority for the specified port(s) in the specified MST instance. (For a given port, the priority setting can be different for different MST instances to which the port may belong.) The priority range for a port in a given MST instance is 0-255. However, this command specifies the priority as a multiplier (0 - 15) of 16. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

(*priority-multiplier*) *x* 16

*For example, if you configure "***2***" as the priority multiplier on a given port in an MST instance, then the actual* **Priority** *setting is 32. Thus, after you specify the port priority multiplier in an instance, the switch displays the actual port priority (and not the multiplier) in the* **show spanning-tree instance < 1..16 >** *or* **show spanning-tree < *port-list* > instance < 1..16 >** *displays. You can view the actual multiplier setting for ports in the specified instance by executing* **show running** *and looking for an entry in this format:*

spanning-tree instance < 1..15 > < *port-list* > priority < *priority-multiplier* >

For example, configuring port A2 with a priority multiplier of "3" in instance 1, results in this line in the **show running** *output:*

```
spanning-tree instance 1 A2 priority 3
```

Syntax: spanning-tree < *port-list* > priority < *priority-multiplier* >

This command sets the priority for the specified port(s) for the IST (that is, Instance 0) of the region in which the switch resides. The "priority" component of the port's "Port Identifier" is set. The Port Identifier is a unique identifier that helps distinguish this switch's ports from all others. It consists of the Priority value with the port number extension—PRIORITY:PORT_NUMBER. A port with a lower value of Port Identifier is more likely to be included in the active topology.

This priority is compared with the priorities of other ports in the IST to determine which port is the root port for the IST instance. The lower the priority value, the higher the priority. The IST root port (or trunk) in a region provides the path to connected regions for the traffic in VLANs assigned to the region's IST instance.

The priority range for a port in a given MST instance is 0-240. However, this command specifies the priority as a multiplier (0 - 15) of 16. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

(*priority-multiplier*) x 16

*For example, configuring "***5***" as the priority multiplier on a given port in the IST instance for a region creates an actual* **Priority** *setting of* **80***. Thus, after you specify the port priority multiplier for the IST instance, the switch displays the actual port priority (and not the multiplier) in the* **show spanning-tree instance ist** *or* **show spanning-tree < *port-list* > instance ist** *displays. You can view the actual multiplier setting for ports in the IST instance by executing* **show running** *and looking for an entry in this format:*

spanning-tree < *port-list* > priority < *priority-multiplier* >

For example, configuring port A2 with a priority multiplier of "2" in the IST instance, results in this line in the **show running** *output:*

```
spanning-tree A2 priority 2
```

Enabling or Disabling Spanning Tree Operation

This command enables or disables spanning tree operation for any spanning tree protocol enabled on the switch. Before using this command to enable spanning tree, ensure that the version you want to use is active on the switch.

Syntax: [no] spanning-tree

Enabling spanning tree with MSTP configured implements MSTP for all physical ports on the switch, according to the VLAN groupings for the IST instance and any other configured instances. Disabling MSTP removes protection against redundant loops that can significantly slow or halt a network.

This command simply turns spanning tree on or off. It does not change the existing spanning tree configuration.

Note

The convergence time for implementing MSTP changes can be disruptive to your network. To minimize such disruption, consider using the **spanning-tree pending** command (refer to the following section on "Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another").

Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another

This operation exchanges the currently active MSTP configuration with the currently pending MSTP configuration. It enables you to implement a new MSTP configuration with minimal network disruption or to exchange MSTP configurations for testing or troubleshooting purposes.

When you configure or reconfigure MSTP, the switch re-calculates the corresponding network paths. This can have a ripple effect throughout your network as adjacent MSTP switches recalculate network paths to support the configuration changes invoked in a single switch. Although MSTP employs rapid spanning-tree operation, the convergence time for implementing MSTP changes can be disruptive to your network. However, by using the **spanning-tree pending** feature, you can set up an MSTP on the switch and then invoke all instances of the new configuration at the same time, instead of one at a time.

Syntax: [no] spanning-tree pending < apply | config-name | config-revision | instance | reset >

This command exchanges the currently active MSTP configuration with the current pending MSTP configuration. Options are as follows:

apply*: Exchanges the currently active MSTP configuration with the pending MSTP configuration.*

config-name*: Specifies the pending MST region name. Must be the same for all MSTP switches in the region. (Default: The switch's MAC address.)*

config-revision: *Specifies the pending MST region configuration revision number. Must be the same for all MSTP switches in the region. (Default: 0).*

instance < *1..16* > **vlan** < *vid | vid-range* >*: Creates the pending instance and assigns one or more VLANs to the instance.*

reset*: Copies the switch's currently active MSTP configuration to the pending configuration. This is useful when you want to experiment with the current MSTP configuration while maintaining an unchanged version.*

To Create a Pending MSTP Configuration. This procedure creates a pending MSTP configuration and exchanges it with the active MSTP configuration:

1. Configure the VLANs you want included in any instances in the new region. When you execute the **pending** command, all VLANs configured on the switch will be assigned to a single pending IST instance unless assigned to other, pending MST instances.(The **pending** command creates the region's IST instance automatically.)
2. Configure MSTP as the spanning-tree protocol, then execute **write mem** and reboot. (The pending option is available only with MSTP enabled.)
3. Configure the pending region **config-name** to assign to the switch.
4. Configure the pending **config-revision** number for the region name.
5. If you want an MST instance other than the IST instance, configure the instance number and assign the appropriate VLANs (VIDs) using the **pending instance** < *1..16* > **vlan** < *vid | vid-range* > command.
6. Repeat step 5 for each additional MST instance you want to configure.

7. To review your pending configuration, use the **show spanning-tree pending** command (see page 4-57).
8. To exchange the currently active MSTP configuration with the pending MSTP configuration, use the **spanning-tree pending apply** command.

MSTP VLAN Configuration Enhancement

The MSTP VLAN configuration enhancement allows you to preconfigure an MSTP regional topology and ensure that the same VLAN ID-to-MSTI assignments exist on each MSTP switch in the region.

Caution

When this software version is installed, the prior VLAN ID-to-MSTI mappings do not change. However, this enhancement is not backward-compatible. If you install a software version prior to this version, and you have configured MSTI entries instances mapped to VLANs, they will be removed from the configuration file when booting to the prior version of software. You must do one of the following if you want to install or reload a prior version of the software:

1. Remove all MSTP mappings from the config file and then reconfigure the instance mapping after you are running the desired software version.
2. Save your current configuration file before updating your software to a new version. If you later reload this older version of the software, you can used this configuration file when you reload the older version. See "How to Save Your Current Configuration" on page 4-47.

The default behavior of the **spanning-tree instance vlan** command changes so that, before a static VLAN is configured or a dynamic VLAN is learned on the switch, you can preconfigure its VLAN ID-to-MSTI mapping. Later, when the VLAN is created, it is automatically assigned to the MSTI to which you had previously mapped it.

By supporting preconfigured VLAN ID-to-MSTI topologies, the VLAN Configuration enhancement provides the following benefits:

- Scalability: In a network design in which you plan to use a large number of VLANs, you can preconfigure identical VLAN ID-to-MSTI mappings on all switches in a single, campus-wide MST region, regardless of the specific VLANs that you later configure on each switch. After the initial VLAN ID-to-MSTI mapping, you can decide on the exact VLANs that you need on each switch.

  All switches in a region must be configured with the same VLAN ID-to-MSTI mappings and the same MSTP configuration identifiers (region name and revision number).

- Flexibility: By preconfiguring identical VLAN ID-to-MSTI mappings on all switches in an MST region, you can combine switches that support different maximum numbers of VLANs.
- Network stability: You can reduce the interruptions in network connectivity caused by the regeneration of spanning trees in the entire network each time a configuration change in VLAN-to-MSTI mapping is detected on a switch. The negative impact on network performance is reduced if all newly created VLANs are pre-mapped to the correct MST instances. Later, VLAN creation and deletion are ignored by MSTP and no interruption in spanning-tree traffic occurs.
- Usability: Dynamically learned GVRP VLANs can be mapped to MSTIs and support MSTP load balancing.

PreConfiguring VLANs in an MST Instance

When you configure an MSTP regional topology, you create multiple spanning-tree instances. Each MST instance provides a fully connected active topology for a particular set of VLANs.

Each switch in an MSTP region is configured with the following set of common parameters:

- Region name (**spanning-tree config-name**)
- Region revision number (**spanning-tree config-revision**)
- Identical VLAN ID-to-MSTI mapping (**spanning-tree instance vlan**)

Each MST instance supports a different set of VLANs. A VLAN that is mapped to an MST instance cannot be a member of another MST instance.

The MSTP VLAN configuration enhancement allows you to ensure that the same VLAN ID-to-MSTI assignments exist on each MSTP switch in a region. Before a static VLAN is configured or a dynamic VLAN is learned on the switch, you can used the **spanning-tree instance vlan** command to map VLANs to each MST instance in the region. Later, when the VLAN is created, the switch automatically assigns it to the MST instance to which you had previously mapped it.

Syntax: [no] spanning-tree instance < 1..16 > vlan < *vid* [*vid..vid*] >
no spanning-tree instance < 1..16 >

Configuring MSTP on the switch automatically configures the IST instance and places all statically and dynamically configured VLANs on the switch into the IST instance. This command creates a new MST instance (MSTI) and moves the VLANs you specify from the IST to the MSTI.

You must map at least one VLAN to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region.

The **no** *form of the command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the* **no** *form of the command deletes the specified MSTI.*

When you remove a VLAN from an MSTI, the VLAN returns to the IST instance, where it can remain or be re-assigned to another MSTI configured in the region.

Note: *The valid VLAN IDs that you can map to a specified MSTI are from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement allows you to preconfigure MSTP topologies before the VLAN IDs associated with each instance exist on a switch.*

When you use preconfigured VLAN ID-to-MSTI topologies, ensure that MSTP switches remain in the same region by mapping all VLAN IDs used in the region to the same MSTIs on each regional switch.

Configuring MSTP Instances with the VLAN Range Option

For the switches covered in this guide, if you use the **spanning-tree instance** command with the VLAN range option, even if the range includes VLANs that are not currently present on the switch, the entire range of VLANs is configured. For example, if VLANs 1, 5, and 7 are currently present and you enter this command:

```
ProCurve(config)# spanning-tree instance 1 vlan 1-10
```

then all the VLANs from 1 through 10 are included, even those VLANs that are not present.

On other ProCurve switches, only the VLANs that are present will be included, that is, only VLANs 1, 5, and 7 would be included. The switch will map these VLANs to MSTP Instance 1, which results in a Configuration Digest that is not the same as the Configuration Digest for the switches running this enhancement. (See Figure 4-10 and Figure 4-11)

Figure 4-10 shows an example of an MSTP instance configured with the VLAN range option. All the VLANs are included in the instance whether they exist or not. Figure 4-11 shows an example of an MSTP instance configured on another ProCurve switch. Only VLANs 1, 5, and 7 are included in the instance.

```
ProCurve(config)# show spanning-tree mst-config

MST Configuration Identifier Information
 MST Configuration Name: MSTP1
 MST Configuration Revision: 1
 MST Configuration Digest: 0x51B7EBA6BEED8702D2BA4497D4367517

 IST Mapped VLANs :

 Instance ID Mapped VLANs
 -------- ---------------
 1        1-10
```

Figure 4-10. An Example of Mapping VLANs with the Range Option where all VLANs are Included

The Configuration Digest value shown in Figure 4-11 is not the same as in Figure 4-10, indicating that these switches do not operate in the same instance.

The Common Spanning Tree (CST) will still have the correct root associations.

```
ProCurve(config)# show spanning-tree mst-config

MST Configuration Identifier Information
 MST Configuration Name: MSTP1
 MST Configuration Revision: 1
 MST Configuration Digest: 0x89D3ADV471668D6D832F6EC4AA9CF4AA

 IST Mapped VLANs :

 Instance ID Mapped VLANs
 -------- ---------------
 1        1, 5, 7
```

Figure 4-11. Example of Mapping VLANs on Other ProCurve Switches

Operating Notes for the VLAN Configuration Enhancement

- Configuring MSTP on the switch automatically configures the Internal Spanning Tree (IST) instance and places all statically and dynamically configured VLANs on the switch into the IST instance. The spanning-tree instance vlan command creates a new MST instance and moves the VLANs you specify from the IST to the MSTI.

  You must map a least one VLAN ID to an MSTI when you create it. You cannot map a VLAN ID to more than one instance. You can create up to 16 MSTIs in a region.

- The **no** form of the spanning-tree instance vlan command removes one or more VLANs from the specified MSTI. If no VLANs are specified, the **no** form of the command deletes the specified MSTI.

  When you remove a VLAN from and MSTI, the VLAN returns to the IST instance, where it can remain or be re-assigned to another MSTI configured in the region.

- If you enter the spanning-tree instance vlan command before a static or dynamic VLAN is configured on the switch to preconfigure VLAN ID-to-MSTI mappings, no error message is displayed. Later, each newly configured VLAN that has already been associated with an MSTI is automatically assigned to the MSTI.

  This new default behavior differs from automatically including configured (static and dynamic) VLANs in the IST instance and requiring you to manually assign individual static VLANs to an MSTI.

- The valid VLAN IDs that you can map to a specified MSTI are from 1 to 4094. The VLAN ID-to-MSTI mapping does not require a VLAN to be already configured on the switch. The MSTP VLAN enhancement allows you to preconfigure MSTP topologies before the VLAN IDs associated with each instance exist on a switch.

- When you use preconfigured VLAN ID-to-MSTI topologies, ensure that MSTP switches remain in the same region by mapping all VLAN IDs used in the region to the same MSTIs on each regional switch.

- The existing MSTP topology configuration is automatically saved. All existing VLAN ID-to-MSTI assignments are maintained on a switch for uninterrupted MSTP network operation.

How to Save Your Current Configuration

You can save your current configuration before updating to a new version of software by following these steps:

1. Enter the **show config files** command to display your current configuration files, as shown in Figure 4-12.

```
ProCurve(config)# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+--------------------
  1 |  *   *   *  | config1
  2 |             | config2
  3 |             |
```

Figure 4-12. An Example of the show config files Command Output

2. To save a configuration file for software version Z.12.43, enter this command:

   ```
   ProCurve(config)# copy config config1 config
   configZ1243.cfg
   ```

   You can choose any name for the saved configuration file that you prefer.

3. Display the configuration files as shown in Figure 4-13. You will see your newly created configuration file listed.

```
ProCurve(config)# show config files

Configuration files:

 id | act pri sec | name
 ---+-------------+----------------------
  1 |  *   *   *  | config1
  2 |             | config2
  3 |             | configK1243.cfg
```

Figure 4-13. A Config File for the Current Software Version is Created

4. Now update your switch to the desired version, for example, Z.12.51. Enter the **show flash** command to see the results. The switch is now running the software version Z.12.51.

```
ProCurve(config)# show flash

Image            Size(Bytes)   Date   Version  Build #
-----            -----------  -------- -------  -------
Primary Image   : 6771179   04/17/08 Z.13.09    304
Secondary Image : 7408949   11/06/08 Z.14.01    123
Boot Rom Version: Z.12.12
Default Boot    : Primary
```

Figure 4-14. Show Flash Command after Upgrading the Switch to a New Version of the Software (Z.12.51)

5. If you want to run the prior software version, Z.12.43 in this example, enter this command:

   ```
   ProCurve(config)# boot system flash secondary config
   configK1243.cfg
   ```

   After rebooting, the switch is running software version Z.12.43 and is using the configuration file that you saved for this software version, configK1243.cfg.

You can also save the Z.12.43 configuration file on a TFTP server. If you wanted to reload the Z.12.43 version of the software again, reload the configuration file before you do the reload.

Displaying MSTP Statistics and Configuration

Command	Page
MSTP Statistics:	
show spanning-tree [< *port-list* >]	below
show spanning-tree [< *port-list* >] detail	4-52
show spanning-tree instance < ist | 1..16 >	4-53
MSTP Configuration	
show spanning-tree [*port-list*] config	4-54
show spanning-tree [port-list] config instance < ist | 1..16 >	4-55
show spanning-tree mst-config	4-56
show spanning-tree pending < < instance | ist > | mst-config >	4-57

SNMP MIB Support for MSTP. MSTP is a superset of the STP/802.1D and RSTP/802.1w protocols and uses the MIB objects defined for these two protocols.

Displaying Global MSTP Status

The following commands display the MSTP statistics for the connections between MST regions in a network.

Syntax: show spanning-tree

This command displays the switch's global and regional spanning-tree status, plus the per-port spanning-tree operation at the regional level. Note that values for the following parameters appear only for ports connected to active devices: **Designated Bridge**, **Hello Time**, **PtP**, *and* **Edge**.

Syntax: show spanning-tree < *port-list* >

This command displays the spanning-tree status for the designated port(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, you would use this command: **show spanning-tree a20-a42,trk1**

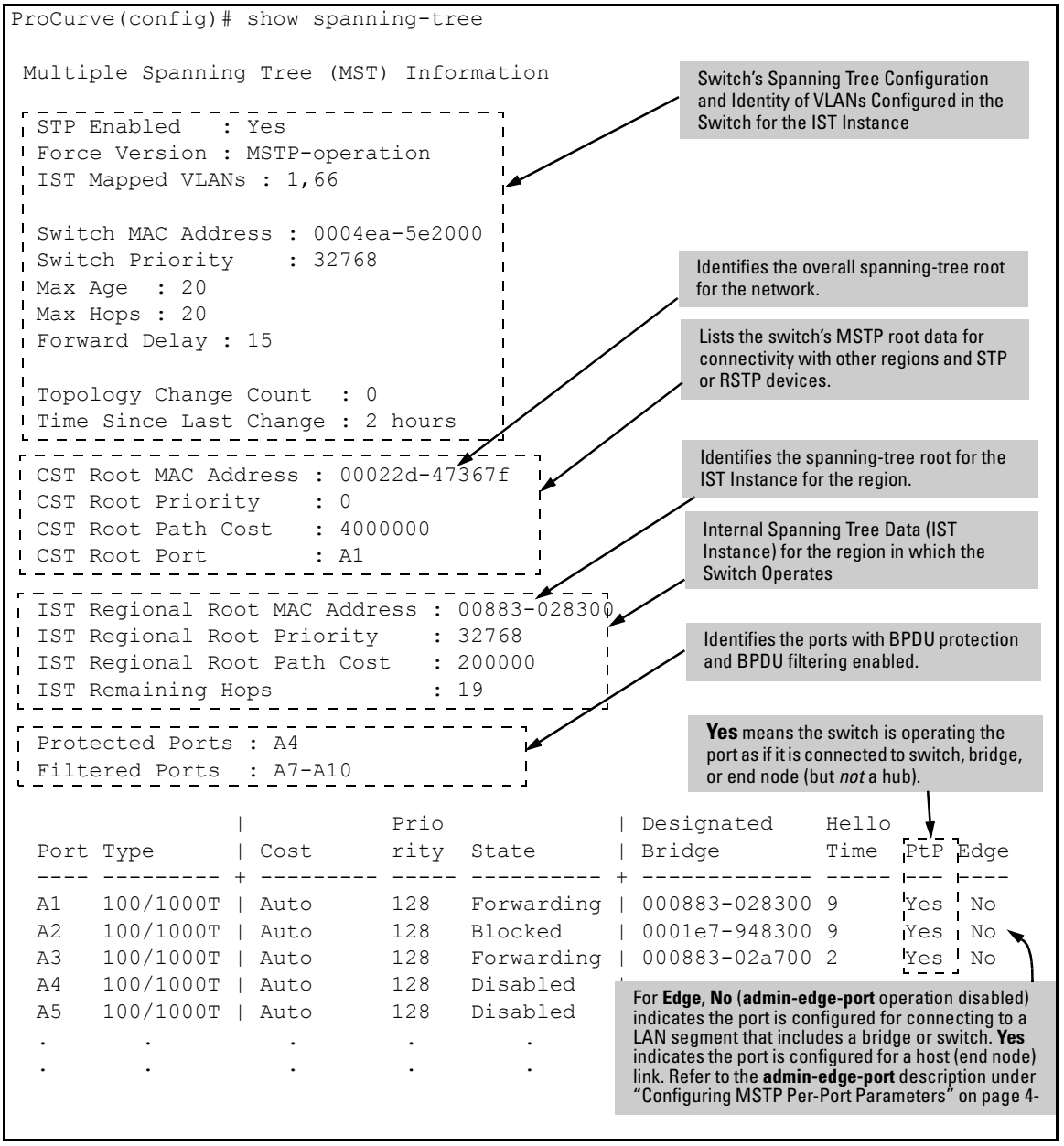

ProCurve(config)# show spanning-tree
Multiple Spanning Tree (MST) Information
STP Enabled : Yes
Force Version : MSTP-operation
IST Mapped VLANs : 1,66
Switch MAC Address : 0004ea-5e2000
Switch Priority : 32768
Max Age : 20
Max Hops : 20
Forward Delay : 15
Topology Change Count : 0
Time Since Last Change : 2 hours
CST Root MAC Address : 00022d-47367f
CST Root Priority : 0
CST Root Path Cost : 4000000
CST Root Port : A1
IST Regional Root MAC Address : 00883-028300
IST Regional Root Priority : 32768
IST Regional Root Path Cost : 200000
IST Remaining Hops : 19
Protected Ports : A4
Filtered Ports : A7-A10
Port Type | Cost Prio rity State | Designated Bridge Hello Time PtP Edge
A1 100/1000T | Auto 128 Forwarding | 000883-028300 9 Yes No
A2 100/1000T | Auto 128 Blocked | 0001e7-948300 9 Yes No
A3 100/1000T | Auto 128 Forwarding | 000883-02a700 2 Yes No
A4 100/1000T | Auto 128 Disabled
A5 100/1000T | Auto 128 Disabled
Switch's Spanning Tree Configuration and Identity of VLANs Configured in the Switch for the IST Instance
Identifies the overall spanning-tree root for the network.
Lists the switch's MSTP root data for connectivity with other regions and STP or RSTP devices.
Identifies the spanning-tree root for the IST Instance for the region.
Internal Spanning Tree Data (IST Instance) for the region in which the Switch Operates
Identifies the ports with BPDU protection and BPDU filtering enabled.
Yes means the switch is operating the port as if it is connected to switch, bridge, or end node (but not a hub).
For Edge, No (admin-edge-port operation disabled) indicates the port is configured for connecting to a LAN segment that includes a bridge or switch. Yes indicates the port is configured for a host (end node) link. Refer to the admin-edge-port description under "Configuring MSTP Per-Port Parameters" on page 4-

Figure 4-15. Example of Common Spanning Tree Status

Displaying Detailed Port Information

The following commands display the MSTP statistics for the connections between MST regions in a network.

Syntax: show spanning-tree detail

This command displays additional parameters concerning the common spanning tree (CST) ports.

Syntax: show spanning-tree < *port-list* > detail

This command displays detailed spanning-tree status for the designated port(s).

.

```
ProCurve# show spanning-tree a9 detail

 Status and Counters - CST Port(s) Detailed Information

 Port                        : A9
 Status                      : Up
 BPDU Filtering              : Yes
 Errant BPUDUs received      : 65
 MST Region Boundary         : Yes
 External Path Cost          : 200000
 External Root Path Cost     : 420021
 Administrative Hello Time   : Use Global
 Operational Hello Time      : 2
 AdminEdgePort               : No
 OperEdgePort                : No
 AdminPointToPointMAC        : Force-True
 OperPointToPointMAC         : Yes
 Aged BPDUs Count            : 0
 Loop-back BPDUs Count       : 0
 TC ACK Flag Transmitted     : 0
 TC ACK Flag Received        : 0

 MST         MST         CFG         CFG         TCN         TCN
 BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx
 ----------- ----------- ----------- ----------- ----------- -----------
 8           28          0           0           0           0
```

Gives information concerning the Common Spanning Tree (CST) only. Use the show spanning-tree instance commands to view counters pertaining to particular IST instances.

Figure 4-16. Example of CST Port Information using Show Spanning Tree Detail Command

Note This command gives information about the CST only. To view details of specific MST Instances, use the **show spanning tree instance** commands.

Displaying Status for a Specific MST Instance

The following commands display the MSTP statistics for a specified MST instance.

Syntax: show spanning-tree instance < ist | 1..16 >

This command displays the MSTP statistics for either the IST instance or a numbered MST instance running on the switch.

Syntax: show spanning-tree instance < ist | 1..16 > detail

This command displays status on all active ports for a specific instance of MSTP.

Syntax: show spanning-tree < *port-list* > instance < ist | 1..16 > detail

This command displays detailed status for the designated port(s) for a specific instance of MSTP.

```
Switch-1(config)# show spanning-tree instance 1

 MST Instance Information

  Instance ID : 1
  Mapped VLANs : 11,22

  Switch Priority          : 32768

  Topology Change Count    : 4
  Time Since Last Change   : 6 secs

  Regional Root MAC Address : 0001e7-948300
  Regional Root Priority    : 32768
  Regional Root Path Cost   : 400000
  Regional Root Port        : A1
  Remaining Hops            : 18
                                                                  Designated
  Port Type       Cost       Priority Role       State          Bridge
  ---- ---------- ---------- -------- ---------- ---------- --------------
  A1   10/100TX   200000     128      Root       Forwarding 000883-028300
  A2   10/100TX   200000     128      Designated Forwarding 000883-02a700
  A3   10/100TX   200000     112      Designated Forwarding 000883-02a700
  A4   10/100TX   Auto       128      Disabled   Disabled
   .       .        .         .          .          .
   .       .        .         .          .          .
   .       .        .         .          .          .
```

Figure 4-17. Example of MSTP Statistics for a Specific Instance on an MSTP Switch

Displaying the MSTP Configuration

Displaying the Global MSTP Configuration. This command displays the switch's basic and MST region spanning-tree configuration, including basic port connectivity settings.

Syntax: show spanning-tree config

The upper part of this output shows the switch's global spanning-tree configuration that applies to the MST region. The port listing shows the spanning-tree port parameter settings for the spanning-tree region operation (configured by the **spanning-tree < *port-list* >** *command). For information on these parameters, refer to "Configuring MSTP Per-Port Parameters" on page 4-26.*

Syntax: show spanning-tree < *port-list* > config

This command shows the same data as the above command, but lists the spanning-tree port parameter settings for only the specified port(s) and/or trunk(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, use this command: **show spanning-tree a20-a24,trk1 config**

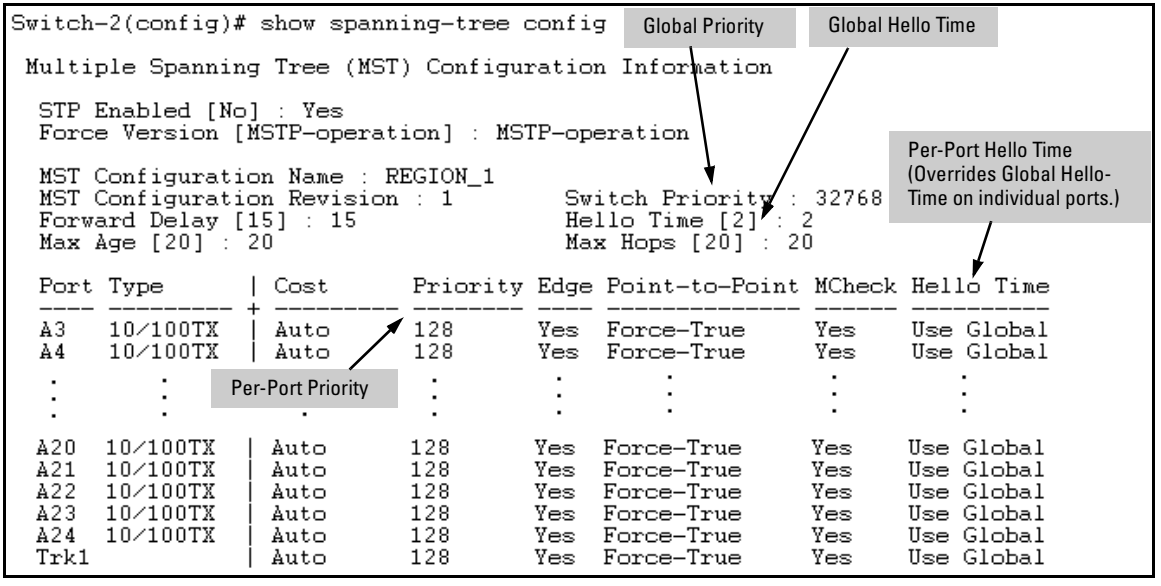

Switch-2(config)# show spanning-tree config
Global Priority
Global Hello Time
Multiple Spanning Tree (MST) Configuration Information
STP Enabled [No] : Yes
Force Version [MSTP-operation] : MSTP-operation
MST Configuration Name : REGION_1
MST Configuration Revision : 1
Switch Priority : 32768
Forward Delay [15] : 15
Hello Time [2] : 2
Max Age [20] : 20
Max Hops [20] : 20
Per-Port Hello Time (Overrides Global Hello-Time on individual ports.)
Port Type | Cost Priority Edge Point-to-Point MCheck Hello Time
A3 10/100TX | Auto 128 Yes Force-True Yes Use Global
A4 10/100TX | Auto 128 Yes Force-True Yes Use Global
Per-Port Priority
A20 10/100TX | Auto 128 Yes Force-True Yes Use Global
A21 10/100TX | Auto 128 Yes Force-True Yes Use Global
A22 10/100TX | Auto 128 Yes Force-True Yes Use Global
A23 10/100TX | Auto 128 Yes Force-True Yes Use Global
A24 10/100TX | Auto 128 Yes Force-True Yes Use Global
Trk1 | Auto 128 Yes Force-True Yes Use Global

Figure 4-18. Example of Displaying the Switch's Global Spanning-Tree Configuration

Displaying Per-Instance MSTP Configurations. These commands displays the per-instance port configuration and current state, along with instance identifiers and regional root data.

Syntax: show spanning-tree config instance < ist | 1..16 >

The upper part of this output shows the instance data for the specified instance. The lower part of the output lists the spanning-tree port settings for the specified instance.

Syntax: show spanning-tree < *port-list* > config instance < ist | 1..16 >

This command shows the same data as the above command, but lists the spanning-tree port parameter settings for only the specified port(s) and/or trunk(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, use this command:

show spanning-tree a20-a24,trk1 config instance 1

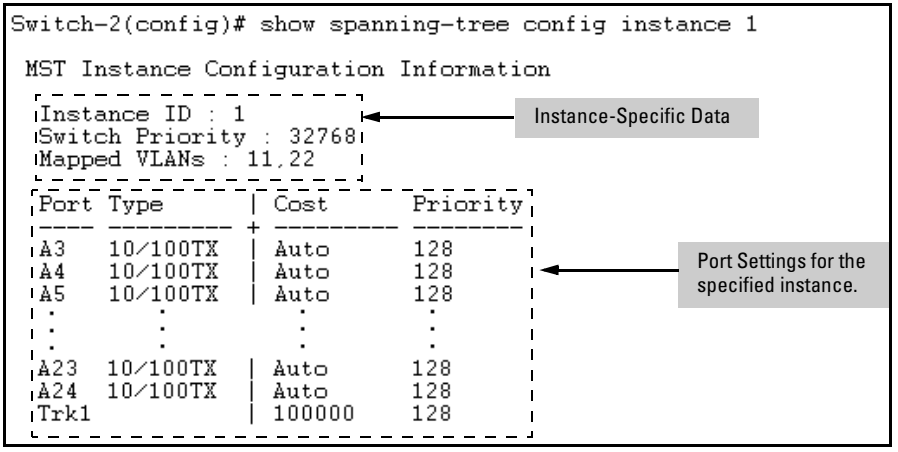

Switch-2(config)# show spanning-tree config instance 1
MST Instance Configuration Information
Instance ID : 1
Switch Priority : 32768
Mapped VLANs : 11,22
Instance-Specific Data
Port Type | Cost Priority
A3 10/100TX | Auto 128
A4 10/100TX | Auto 128
A5 10/100TX | Auto 128
A23 10/100TX | Auto 128
A24 10/100TX | Auto 128
Trk1 | 100000 128
Port Settings for the specified instance.

Figure 4-19. Example of the Configuration Listing for a Specific Instance

Displaying the Region-Level Configuration in Brief. This command output is useful for quickly verifying the allocation of VLANs in the switch's MSTP configuration and for viewing the configured region identifiers.

Syntax: show spanning-tree mst-config

This command displays the switch's regional configuration.

Note: *The switch computes the* ***MSTP Configuration Digest*** *from the VID to MSTI configuration mappings on the switch itself. As required by the 802.1s standard, all MSTP switches within the same region must have the same VID to MSTI assignments, and any given VID can be assigned to either the IST or one of the MSTIs within the region. Thus, the MSTP Configuration Digest must be identical for all MSTP switches intended to belong to the same region. When comparing two MSTP switches, if their Digest identifiers do not match, then they cannot be members of the same region.*

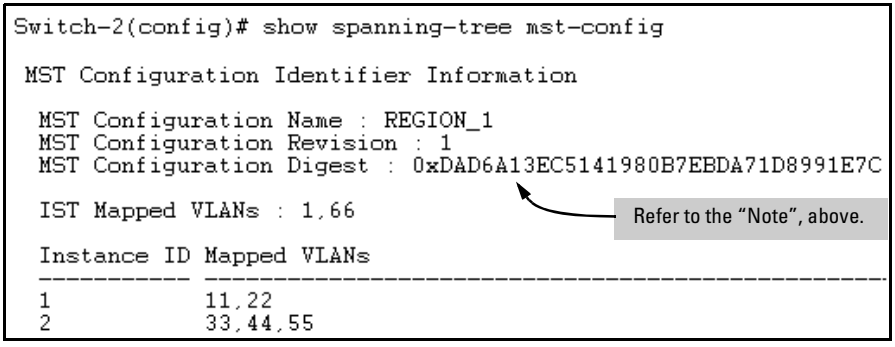

Switch-2(config)# show spanning-tree mst-config
MST Configuration Identifier Information
MST Configuration Name : REGION_1
MST Configuration Revision : 1
MST Configuration Digest : 0xDAD6A13EC5141980B7EBDA71D8991E7C
IST Mapped VLANs : 1,66
Refer to the "Note", above.
Instance ID Mapped VLANs
1 11,22
2 33,44,55

Figure 4-20. Example of a Region-Level Configuration Display

Displaying the Pending MSTP Configuration. This command displays the MSTP configuration the switch will implement if you execute the spanning-tree pending apply command (Refer to "Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another" on page 4-40.)

Syntax: show spanning-tree pending < instance | mst-config >

instance < 1..16 | ist >

Lists region, instance I.D. and VLAN information for the specified, pending instance.

mst-config

Lists region, IST instance VLAN(s), numbered instances, and assigned VLAN information for the pending MSTP configuration.

```
ProCurve# show spanning-tree pending instance 1

 Pending MST Instance Configuration Information

  MST Configuration Name : New-Version_01
  MST Configuration Revision : 10
  Instance ID : 1
  Mapped VLANs : 1,22



Switch-1(config)# show spanning-tree pending mst-config

 Pending MST Configuration Identifier Information

  MST Configuration Name : New-Version_01
  MST Configuration Revision : 10

  IST Mapped VLANs : 11,33

  Instance ID Mapped VLANs
  ----------- ----------------------------------------------
  1           1,22
```

Figure 4-21. Example of Displaying a Pending Configuration

Troubleshooting an MSTP Configuration

Command	Page
show spanning-tree root-history	4-58
show spanning-tree debug counters	4-61
show spanning-tree debug-counters instance < *instance-id* >	4-62
show spanning-tree debug-counters instance < *instance-id* > ports <*port-list*>	4-64

This section describes the **show spanning-tree** commands that you can use to monitor, troubleshoot, and debug the operation of a multiple-instance spanning-tree configuration in your network.

Note that the **show spanning-tree** commands described in this section allow you to troubleshoot MSTP activity in your network by focusing on increasingly specific levels of operation. For example, you can display debug information for:

- All MST instances
- All ports used in one MST instance
- A specific port or several ports used in one MST instance

Also, you can display the change history for the root (bridge) switch used as the single forwarding path for:

- All MST regions, STP bridges, and RSTP bridges in an STP network
- All VLANs on MSTP switches in a region
- All VLANs on MSTP switches in an MST instance

Displaying the Change History of Root Bridges

The **show spanning-tree root-history** command allows you to display change history information (up to 10 history entries) for a specified root bridge in any of the following MSTP topologies:

- Common Spanning Tree (**cst**): Provides connectivity in a bridged network between MST regions, STP LANs, and RSTP LANs.
- Internal Spanning Tree (**ist**): Provides connectivity within an MST region for VLANs associated with the default Common and Internal Spanning Tree (CIST) instance in your network (VLANs that have not been mapped to an MST instance).

- MST Instance (**mst**): Connects all static and (starting from release 13.*x.x*) dynamic VLANs assigned to a multiple spanning-tree instance.

Syntax: show spanning-tree root-history <cst | ist | mst <*instance-id*>>

This command displays the change history for the root bridge in the specified MSTP topology.

The **cst** *parameter displays the change history for the root bridge of a spanning-tree network, including MST regions and STP and RSTP bridges.*

The **ist** *parameter displays the change history for the root bridge in the IST instance of an MST region.*

The **mst** *<instance-id> parameter displays the change history for the root bridge in an MST instance, where <instance-id> is an ID number from 1 to 16.*

Use the **show spanning-tree root-history** command to view the number and dates of changes in the assignment of a root bridge. Possible intrusion into your MST network may occur if an unauthorized external device gains access to a spanning tree by posing as the root device in a topology. To prevent an MST port connected to the device from being selected as the root port in a topology, use the **spanning-tree root-guard** command.

The following examples show sample output of the **show spanning-tree root-history** command for different MSTP topologies. Note that in each example, the root bridge ID is displayed in the format:
<*priority*:*mac-address*>

Where:

- <*priority*> is the MSTP switch priority calculated for one of the following:
  - The IST (regional) root switch using the **spanning-tree priority** command
  - An MSTI root switch using the **spanning-tree instance priority** command
- <*mac-address*> is the MAC address of the root (bridge) switch.

```
ProCurve(config)# show spanning-tree root-history cst

 Status and Counters - CST Root Changes History

  MST Instance ID        : 0
  Root Changes Counter   : 2
  Current Root Bridge ID : 32768:000883-024500

  Root Bridge ID      Date     Time
  ------------------- -------- --------
  32768:000883-024500 02/09/07 17:40:59
  36864:001279-886300 02/09/07 17:40:22
```

Identifies the root bridge of the common spanning tree in a bridged network that connects different MST regions and STP or RSTP devices.

Figure 4-22. Example of show spanning-tree root-history cst Command Output

```
ProCurve(config)# show spanning-tree root-history ist

 Status and Counters - IST Regional Root Changes History

  MST Instance ID        : 0
  Root Changes Counter   : 2
  Current Root Bridge ID : 32768:000883-024500

  Root Bridge ID      Date     Time
  ------------------- -------- --------
  32768:000883-024500 02/09/07 17:40:59
  36864:001279-886300 02/09/07 17:40:22
```

Identifies the root bridge of the internal spanning tree in an MST region.

Figure 4-23. Example of show spanning-tree root-history ist Command Output

```
ProCurve(config)# show spanning-tree root-history mst 2

 Status and Counters - MST Instance Regional Root Changes History

  MST Instance ID        : 2
  Root Changes Counter   : 2
  Current Root Bridge ID : 32770:000883-024500

  Root Bridge ID      Date     Time
  ------------------- -------- --------
  32770:000883-024500 02/09/07 17:40:59
  32770:001279-886300 02/09/07 17:40:22
```

Identifies the root bridge of an MST instance in an MST region.

Figure 4-24. Example of show spanning-tree root-history msti Command Output

Displaying Debug Counters for All MST Instances

The **show spanning-tree debug-counters** command allows you to display the aggregate values of all MSTP debug counters that are maintained on a switch. These aggregate values are a summary of the information collected from all ports and from all spanning-tree instances that forward traffic on switch ports.

Use the displayed diagnostic information to globally monitor MSTP operation on a per-switch basis.

Syntax: show spanning-tree debug-counters

This command displays debug counters for MSTP activity on all ports configured for VLANs used in spanning-tree instances.

The following example shows sample output of the **show spanning-tree debug-counters** command for all ports. For a description of each counter, refer to Table 4-1 on page 4-66.

```
ProCurve(config)# show spanning-tree debug-counters

 Status and Counters - MSTP Bridge Common Debug Counters Information

  Counter Name                      Aggregated Value Collected From
  --------------------------------- ---------------- --------------
  Invalid BPDUs                     0                CIST
  Errant BPDUs                      170927           CIST
  MST Config Error BPDUs            0                CIST
  Looped-back BPDUs                 0                CIST
  Starved BPDUs/MSTI MSGs           0                CIST/MSTIs
  Exceeded Max Age BPDUs            0                CIST
  Exceeded Max Hops BPDUs/MSTI MSGs 0                CIST/MSTIs
  Topology Changes Detected         2                CIST/MSTIs
  Topology Changes Tx               6                CIST/MSTIs
  Topology Changes Rx               4                CIST/MSTIs
  Topology Change ACKs Tx           0                CIST
  Topology Change ACKs Rx           0                CIST
  TCN BPDUs Tx                      0                CIST
  TCN BPDUs Rx                      0                CIST
  CFG BPDUs Tx                      0                CIST
  CFG BPDUs Rx                      0                CIST
  RST BPDUs Tx                      0                CIST
  RST BPDUs Rx                      0                CIST
  MST BPDUs/MSTI MSGs Tx            10               CIST/MSTIs
  MST BPDUs/MSTI MSGs Rx            341802           CIST/MSTIs
```

Figure 4-25. Example of show spanning-tree debug-counters Command Output

Displaying Debug Counters for One MST Instance

The **show spanning-tree debug-counters instance** command allows you to display the aggregate values of all MSTP debug counters maintained on a switch for a specified spanning-tree instance. These aggregate values are a summary of information collected from all ports that have VLANs assigned to the specified instance.

Use the **show spanning-tree debug-counters instance** command to troubleshoot the global MSTP diagnostic information displayed in **show spanning-tree debug-counters** command output when you suspect unauthorized MSTP activity in a specific MST instance.

Syntax: show spanning-tree debug-counters instance <*instance-id*>

This command displays debug counters for MSTP activity on all ports configured for VLANs in the specified MST instance. The valid values for **instance** <*instance-id*> *are from 0 to 16:*

- *0 specifies the default MST (CIST) instance.*
- *1 to 16 specify a multiple spanning-tree (MST) instance.*

The following example shows sample output of the **show spanning-tree debug-counters instance** command when applied to the Common and Internal Spanning Tree (CIST) instance (default MST instance 0) in the network. For a description of each counter, refer to Table 4-1 on page 4-66.

```
ProCurve(config)# show spanning-tree debug-counters instance 0

 Status and Counters - CIST Common Debug Counters Information

  MST Instance ID : 0

  Counter Name                     Aggregated Value Collected From
  -------------------------------- ---------------- --------------
  Invalid BPDUs                    0                Ports
  Errant BPDUs                     172603           Ports
  MST Config Error BPDUs           0                Ports
  Looped-back BPDUs                0                Ports
  Starved BPDUs                    0                Ports
  Exceeded Max Age BPDUs           0                Ports
  Exceeded Max Hops BPDUs          0                Ports
  Topology Changes Detected        1                Ports
  Topology Changes Tx              3                Ports
  Topology Changes Rx              2                Ports
  Topology Change ACKs Tx          0                Ports
  Topology Change ACKs Rx          0                Ports
  TCN BPDUs Tx                     0                Ports
  TCN BPDUs Rx                     0                Ports
  CFG BPDUs Tx                     0                Ports
  CFG BPDUs Rx                     0                Ports
  RST BPDUs Tx                     0                Ports
  RST BPDUs Rx                     0                Ports
  MST BPDUs Tx                     5                Ports
  MST BPDUs Rx                     172577           Ports
```

Figure 4-26. Example of show spanning-tree debug-counters instance Command Output for All Ports in the CIST Instance

Displaying Debug Counters for Ports in an MST Instance

The **show spanning-tree debug-counters instance ports** command allows you to display the aggregate values of all MSTP debug counters maintained on one or more ports used by a specified spanning-tree instance. These aggregate values are a summary of information collected from the specified ports that have VLANs assigned to the specified instance.

Use the **show spanning-tree debug-counters instance ports** command to troubleshoot at a finer level the more general MSTP diagnostic information displayed in **show spanning-tree debug-counters instance** command output when you suspect unauthorized MSTP activity on one or more MST ports in an MST instance.

Syntax: show spanning-tree debug-counters instance <*instance-id*> ports <*port-list*>

This command displays debug counters for MSTP activity on the specified ports configured for VLANs in the specified MST instance.

The valid values for **instance** <*instance-id*> *are from 0 to 16:*

- *0 specifies the default MST (CIST) instance.*
- *1 to 16 specify an MST instance.*

The **ports** <*port-list*> *parameter specifies one or more MST ports or trunk ports.*

In the port list, enter a series of ports by separating the first and last ports in the series with a dash (-); for example, **a2-a8** *or* **trk1-trk3**. *Separate individual ports and series of ports with a comma; for example,* **a2-a8**, **a20**, **trk1, trk4-trk5**.

The following examples shows sample output of the **show spanning-tree debug-counters instance ports** command for both the CIST (default MST instance 0) and an MST instance (instance 2) on port A15. For a description of each counter, refer to Table 4-1 on page 4-66.

```
ProCurve(config)# show spanning-tree debug-counters instance 0 ports a15

 Status and Counters - CIST Port(s) Debug Counters Information

  MST Instance ID : 0
  Port : A15

  Counter Name                 Value      Last Updated
  ---------------------------- ---------- -----------------
  Invalid BPDUs                0
  Errant BPDUs                 0
  MST Config Error BPDUs       0
  Looped-back BPDUs            0
  Starved BPDUs                0
  Exceeded Max Age BPDUs       0
  Exceeded Max Hops BPDUs      0
  Topology Changes Detected    1          02/09/07 17:40:59
  Topology Changes Tx          3          02/09/07 17:41:03
  Topology Changes Rx          2          02/09/07 17:41:01
  Topology Change ACKs Tx      0
  Topology Change ACKs Rx      0
  TCN BPDUs Tx                 0
  TCN BPDUs Rx                 0
  CFG BPDUs Tx                 0
  CFG BPDUs Rx                 0
  RST BPDUs Tx                 0
  RST BPDUs Rx                 0
  MST BPDUs Tx                 5          02/09/07 17:41:03
  MST BPDUs Rx                 173540     02/13/07 18:05:34
```

Figure 4-27. Example of show spanning-tree debug-counters instance ports Command Output for One Port in the CIST Instance

```
ProCurve(config)# show spanning-tree debug-counters instance 2 ports a15

 Status and Counters - MSTI Port(s) Debug Counters Information

  MST Instance ID : 2
  Port : A15

  Counter Name                 Value      Last Updated
  ---------------------------- ---------- -----------------
  Starved MSTI MSGs            0
  Exceeded Max Hops MSTI MSGs  0
  Topology Changes Detected    1          02/09/07 17:40:59
  Topology Changes Tx          3          02/09/07 17:41:03
  Topology Changes Rx          2          02/09/07 17:41:01
  MSTI MSGs Tx                 5          02/09/07 17:41:03
  MSTI MSGs Rx                 173489     02/13/07 18:03:52
```

Figure 4-28. Example of show spanning-tree debug-counters instance ports Command Output for One Port in an MST Instance

Field Descriptions in MSTP Debug Command Output

Table 4-1 contains descriptions of the debugging information displayed in the output of **show spanning-tree debug-counters** commands.

Table 4-1. MSTP Debug Command Output: Field Descriptions

Field	Description
Invalid BPDUs	Number of received BPDUs that failed standard MSTP (802.1Q-REV/D5.0 14.4) validation checks and were dropped. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Errant BPDUs	Number of received BPDUs that were dropped on a port that is configured to not expect BPDU packets. This counter is maintained by the CIST (default MST instance 0 in the network) on a per-port basis and is incremented each time a BPDU packet is received on a port configured with the BPDU filter to ignore incoming BPDU packets (**spanning-tree bpdu-filter** command) or the BPDU protection feature to disable the port when BPDU packets are received (**spanning-tree bpdu-protection** command).

Field	Description
MST Config Error BPDUs	Number of BPDUs received from a neighbor bridge with inconsistent MST configuration information. For example, BPDUs from a transmitting bridge may contain the same MST configuration identifiers (region name and revision number) and format selector as the receiving bridge, but the value of the Configuration Digest field (VLAN ID assignments to regional IST and MST instances) is different. This difference indicates a probable configuration error in MST region settings on the communicating bridges. The received BPDU is still processed by MSTP. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Looped-back BPDUs	Number of times a port has received self-sent BPDU packets as the result of an external loop condition in which the BPDUs were looped back to the originating transmission port. The received BPDU is still processed by MSTP and the port changes to a blocked state. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Starved BPDUs	Number of times that no BPDUs are received within the scheduled interval (three times the Hello Time value configured with the **spanning-tree hello-time** command) from a downstream CIST-designated peer port on the CIST root, alternate, or backup port. As a result, the "starved" port triggers a spanning-tree topology regeneration. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Starved MSTI MSGs	Number of times that no BPDUs are received within the scheduled interval (three times the Hello Time value configured with the **spanning-tree hello-time** command) from a downstream MSTI-designated peer port on the MSTI root, alternate, or backup port. As a result, the "starved" port triggers a spanning-tree topology regeneration. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Exceeded Max Age BPDUs	Number of times that a BPDU packet is received from a bridge external to the MST region with a Message Age value greater than the configured value of the Max Age parameter (**spanning-tree maximum age** command). This may occur if the receiving bridge is located too far from the root bridge (beyond the configured size of the spanning-tree domain on the root bridge) or if a BPDU packet with invalid root information is continuously circulating between bridges in a spanning-tree domain and needs to be aged out. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Exceeded Max Hops BPDUs	Number of times that a BPDU packet is received from a bridge internal to the MST region with a CIST Remaining Hops value less than or equal to 1. This may occur if the receiving bridge is located too far from the CIST regional root bridge (beyond the configured size of the MST region on the CIST regional root bridge) or if a PDU packet with invalid CIST regional root bridge information is continuously circulating between bridges in the MST Region and needs to be aged out. This counter is maintained by the CIST (default MST instance 0 in the region) on a per-port basis.

Field	Description
Exceeded Max Hops MSTI MSGs	Number of times that an MSTI MSG packet is received from a bridge internal to the MST region with an MSTI Remaining Hops value less than or equal to 1. This may occur if the receiving bridge is located too far from the MSTI regional root bridge (beyond the configured size of the MST region on the MSTI regional root bridge) or if a BPDU packet with invalid MSTI regional root bridge information is continuously circulating between bridges in an MST region and needs to be aged out. This counter is maintained on a per-MSTI per-port basis.
Topology Changes Detected	Number of times that a Topology Change event is detected by the CIST or MSTI port and the port triggers a topology change propagation throughout the network. A Topology Change event occurs when a non-edge port enters forwarding state. This counter is maintained on a per-CIST per-port and on a per-MSTI per-port basis.
Topology Changes Tx	Number of times that Topology Change information is propagated (sent out) through the port to the rest of the network. For a CIST port, the counter is the number of times that a CFG, RST or MST BPDU with the TC flag set is transmitted out of the port. For an MSTI port, the counter is the number of times that a MSTI configuration message with the TC flag set is transmitted out of the port. This counter is maintained on a per-CIST per-port and on a per-MSTI per-port bases.
Topology Changes Rx	Number of times that Topology Change information is received from the peer port. For a CIST port, the counter is the number of times that a CFG, RST or MST BPDU with the TC flag set is received. For an MSTI port, the counter is the number of times that an MSTI configuration message with the TC flag set is received. This counter is maintained on a per-CIST per-port and on a per-MSTI per-port basis.
Topology Change ACKs Tx	Number of times that the Topology Change acknowledgement is transmitted through the port (number of CFG, RST or MST BPDUs transmitted with the Topology Change Acknowledge flag set). This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
Topology Change ACKs Rx	Number of times the Topology Change acknowledgement is received on the port (number of CFG, RST or MST BPDUs received with the Topology Change Acknowledge flag set). This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
TCN BPDUs Tx	Number of Topology Change Notification BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
TCN BPDUs Rx	Number of Topology Change Notification BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
CFG BPDUs Tx	Number of (802.1D) Configuration BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
CFG BPDUs Rx	Number of (802.1D) Configuration BPDUs that are received on the port. This counter maintained by the CIST (default MST instance 0) on a per-port basis.

Field	Description
RST BPDUs Tx	Number of (802.1w) RST BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
RST BPDUs Rx	Number of (802.1w) RST BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MST BPDUs Tx	Number of (802.1s) MST BPDUs that are transmitted through the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MST BPDUs Rx	Number of (802.1s) MST BPDUs that are received on the port. This counter is maintained by the CIST (default MST instance 0) on a per-port basis.
MSTI MSGs Tx	Number of times that a configuration message for a specific MSTI was encoded in (802.1s) MST BPDUs that are transmitted through the port. This counter is maintained on a per-MSTI per-port basis.
MSTI MSGs Rx	Number of times that the MSTI detected a configuration message destined to the MSTI in (802.1s) MST BPDUs received on the port. This counter is maintained on a per-MSTI per-port basis.

Troubleshooting MSTP Operation

Table 4-2. Troubleshooting MSTP Operation

Problem	Possible Cause
Duplicate packets on a VLAN, or packets not arriving on a LAN at all.	The allocation of VLANs to MSTIs may not be identical among all switches in a region.
A switch intended to operate in a region does not receive traffic from other switches in the region.	An MSTP switch intended for a particular region may not have the same configuration name or region revision number as the other switches intended for the same region. The MSTP configuration name (**spanning-tree config-name** command) and MSTP configuration revision number (**spanning-tree config-revision** command) must be identical on all MSTP switches intended for the same region. Another possible cause is that the set of VLANs and VLAN ID-to-MSTI mappings (**spanning-tree instance vlan** command) configured on the switch may not match the set of VLANs and VLAN ID-to-MSTI mappings configured on other switches in the intended region.

Loop Protection

In cases where spanning tree cannot be used to prevent loops at the edge of the network, loop protection may provide a suitable alternative. Unlike spanning tree, however, loop protection is not a comprehensive loop detection feature and should only be enabled on untagged edge ports, that is, ports that connect to unmanaged switches and/or clients at the edge of the network.

The cases where loop protection might be chosen ahead of spanning tree to detect and prevent loops are as follows:

- **On ports with client authentication**. When spanning tree is enabled on a switch that use 802.1X, Web authentication, and MAC authentication, loops may go undetected. For example, spanning tree packets that are looped back to an edge port will not be processed because they have a different broadcast/multicast MAC address from the client-authenticated MAC address. To ensure that client-authenticated edge ports get blocked when loops occur, you should enable loop protection on those ports.
- **On ports connected to unmanaged devices**. Spanning tree cannot detect the formation of loops where there is an unmanaged device on the network that does not process spanning tree packets and simply drops them. Loop protection has no such limitation, and can be used to prevent loops on unmanaged switches.

Figure 4-29 shows examples where loop protection can be used.

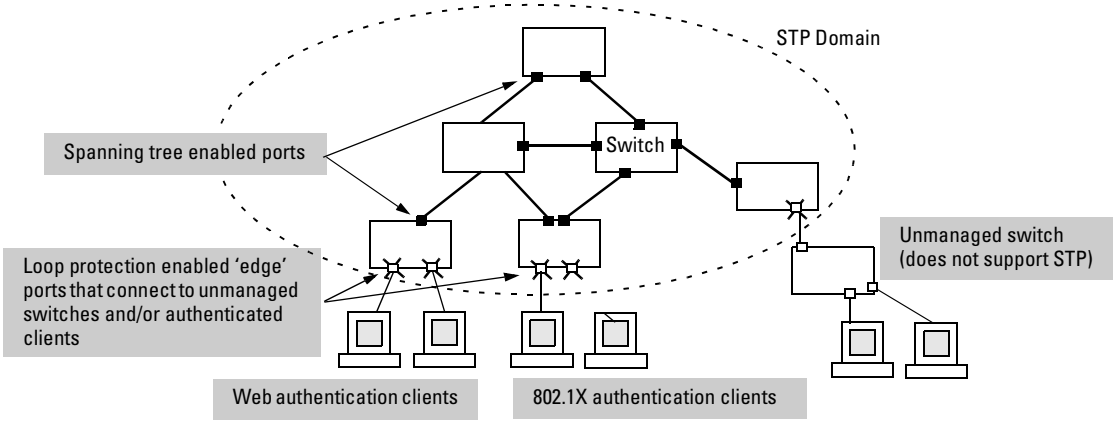

STP Domain
Spanning tree enabled ports
Switch
Unmanaged switch
(does not support STP)
Loop protection enabled 'edge' ports that connect to unmanaged switches and/or authenticated clients
Web authentication clients
802.1X authentication clients

Figure 4-29. Examples of Loop Protection Enabled in Preference to STP

Configuring Loop Protection

Loop protection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet on a port that has a **receiver-action** of **send-disable** configured, it shuts down the port from which the packet was sent.

To enable loop protection:

1. Enter the **loop-protect** command and specify the port(s) on which loop protection should be enabled. For example:

   ```
   ProCurve(config)# loop-protect 1-4
   ```

2. Specify a **receiver-action** of **send-disable** to shut down the port in the event of a loop. For example:

   ```
   ProCurve(config)# loop-protect 1 receiver-action send-
   disable
   ```

Syntax: [no] loop-protect <port-list> [receiver-action <send-disable | no-disable>] | [transmit-interval <1-10>] | [disable-timer <0-604800>] | [trap loop-detected]

Allows you to configure per-port loop protection on the switch.

[receiver-action <send-disable | no-disable>]

Sets the action to be taken when a loop is detected on the specified port or ports. The port that receives the loop protection packet determines what action is taken. If send-disable is configured, the port that transmitted the packet is disabled. If no-disable is configured, the port is not disabled when a loop is detected.
Default: send-disable

[trap loop-detected]

Allows you to configure loop protection traps for SNMP indicating when a loop has been detected on a port.

[disable-timer <0-604800>]

How long (in seconds) a port is disabled when a loop has been detected. A value of zero disables the auto re-enable function.
Default: Timer is disabled

[transmit-interval <1-10>]

Allows you to configure the time in seconds between the transmission of loop protection packets.
Default: 5 seconds

Notes

- The **receiver-action** option can be configured on a per-port basis and can only be enabled after loop protection has been enabled on the port. All other configuration options (**disable-timer**, **trap loop-detected**, and **transmit interval**) are global.
- The **trap** option refers to a SNMP trap.
- Regardless of how the **receiver-action** and **trap** options are configured, all detected loops will be logged in the switch's event log.
- The **no loop-protect** *<port>* command will not remove a receive-action configuration line from the running configuration unless this option is set to **receive-action send-disable**.

Viewing Loop Protection Status

To display information about ports with loop protection enabled, enter the **show loop-protect** command.

Syntax: show loop-protect *<port-list>*

Displays the loop protection status. If no ports are specified, the information is displayed only for the ports that have loop protection enabled.

For example:

```
ProCurve(config)# show loop-protect 1-4

 Status and Counters - Loop Protection Information

 Transmit Interval (sec)  : 5
 Port Disable Timer (sec) : 5
 Loop Detected Trap       : Enabled


      Loop        Loop      Loop       Time              Rx           Port
 Port Protection  Detected  Count      Since Last Loop   Action       Status
 ---- ----------- --------- ---------- ----------------- ------------ --------
 1    Yes          No        0                           send-disable Up
 2    Yes          No        0                           send-disable Up
 3    Yes          No        0                           send-disable Up
 4    Yes          No        0                           send-disable Up
```

Figure 4-30. Example of Show Loop-Protect Display

5

Quality of Service (QoS): Managing Bandwidth More Effectively

Contents

Introduction 5-3
- Terminology 5-6
- Overview 5-7
- Classifiers for Prioritizing Outbound Packets 5-10
  - Packet Classifiers and Evaluation Order 5-10

Preparation for Configuring QoS 5-11
- Preserving 802.1p Priority 5-11
- Steps for Configuring QoS on the Switch 5-11
- Viewing the QoS Configuration 5-13
  - No Override 5-13

Using QoS Classifiers to Configure Quality of Service for Outbound Traffic 5-14
- QoS IP Type-of-Service (ToS) Policy and Priority 5-15
  - Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits 5-16
  - Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP 5-17
  - Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices 5-21
  - Details of QoS IP Type-of-Service 5-24
- QoS Source-Port Priority 5-27
  - Assigning a Priority Based on Source-Port 5-27
  - Assigning a DSCP Policy Based on the Source-Port 5-29

Differentiated Services Codepoint (DSCP) Mapping 5-33
- Default Priority Settings for Selected Codepoints 5-34
  - Quickly Listing Non-Default Codepoint Settings 5-34
- Notes on Changing a Priority Setting 5-36

Error Messages caused by DSCP Policy Changes 5-36
Example of Changing the Priority Setting on a Policy When One or More Classifiers Are Currently Using the Policy . 5-37
QoS Queue Configuration 5-40
QoS Operating Notes and Restrictions 5-41
IP Multicast (IGMP) Interaction with QoS 5-43

Introduction

QoS Feature	Default	Page Reference
IP Type-of-Service Priority	Disabled	page 5-15
Source-Port Priority	Disabled	page 5-27
DSCP Policy Table	Various	page 5-33
Queue Configuration	4 Queues	page 5-40

As the term suggests, *network policy* refers to the network-wide controls you can implement to:

- Ensure uniform and efficient traffic handling throughout your network, while keeping the most important traffic moving at an acceptable speed, regardless of current bandwidth usage.
- Exercise control over the priority settings of inbound traffic arriving in and travelling through your network.

Adding bandwidth is often a good idea, but it is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

When (not *if*) network congestion occurs, it is important to move traffic on the basis of relative importance. However, without *Quality of Service* (QoS) prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. That is, without QoS, most traffic received by the switch is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization’s mission.

This section gives an overview of QoS operation and benefits, and describes how to configure QoS in the console interface.

Quality of Service is a general term for classifying and prioritizing traffic throughout a network. That is, QoS enables you to establish an end-to-end traffic priority policy to improve control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first. For example, you can use Quality of Service to:

- Upgrade or downgrade traffic from various servers.
- Control the priority of traffic from dedicated VLANs or applications.
- Change the priorities of traffic from various segments of your network as your business needs change.
- Set priority policies in edge switches in your network to enable traffic-handling rules across the network.

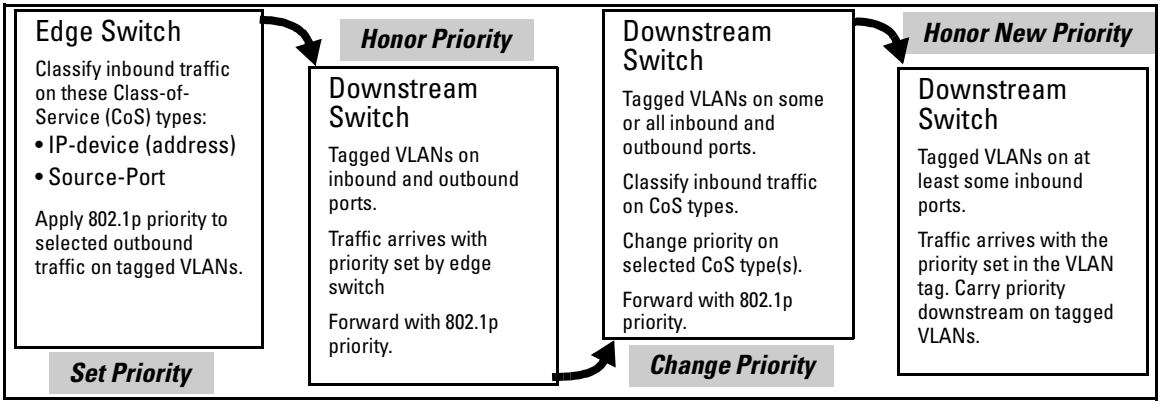

Edge Switch
Classify inbound traffic on these Class-of-Service (CoS) types:
• IP-device (address)
• Source-Port
Apply 802.1p priority to selected outbound traffic on tagged VLANs.
Set Priority
Honor Priority
Downstream Switch
Tagged VLANs on inbound and outbound ports.
Traffic arrives with priority set by edge switch
Forward with 802.1p priority.
Downstream Switch
Tagged VLANs on some or all inbound and outbound ports.
Classify inbound traffic on CoS types.
Change priority on selected CoS type(s).
Forward with 802.1p priority.
Change Priority
Honor New Priority
Downstream Switch
Tagged VLANs on at least some inbound ports.
Traffic arrives with the priority set in the VLAN tag. Carry priority downstream on tagged VLANs.

Figure 5-1. Example of 802.1p Priority Based on CoS (Class-of-Service) Types and Use of VLAN Tags

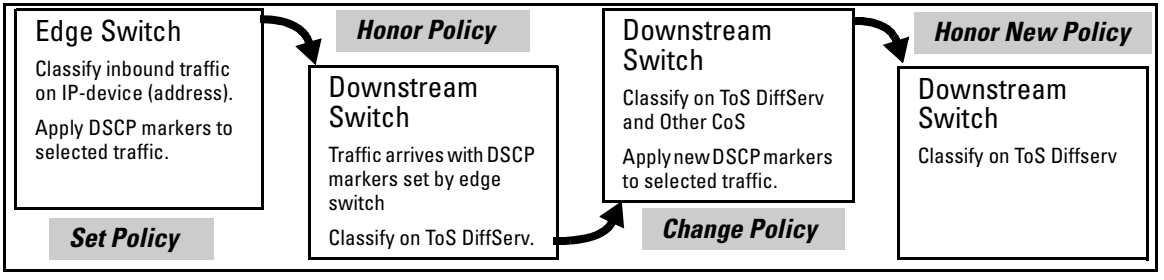

Edge Switch
Classify inbound traffic on IP-device (address).
Apply DSCP markers to selected traffic.
Set Policy
Honor Policy
Downstream Switch
Traffic arrives with DSCP markers set by edge switch
Classify on ToS DiffServ.
Downstream Switch
Classify on ToS DiffServ and Other CoS
Apply new DSCP markers to selected traffic.
Change Policy
Honor New Policy
Downstream Switch
Classify on ToS Diffserv

Figure 5-2. Example Application of Differentiated Services Codepoint (DSCP) Policies

At the edge switch, QoS classifies certain traffic types and in some cases applies a DSCP policy. At the next hop (downstream switch) QoS honors the policies established at the edge switch. Further downstream, another switch may reclassify some traffic by applying new policies, and yet other downstream switches can be configured to honor the new policies.

QoS is implemented in the form of rules or policies that are configured on the switch. While you can use QoS to prioritize only the outbound traffic while it is moving through the switch, you derive the maximum benefit by using QoS in an 802.1Q VLAN environment (with 802.1p priority tags) or in an untagged VLAN environment (with DSCP policies) where QoS can set priorities that downstream devices can support without re-classifying the traffic.

By prioritizing traffic, QoS supports traffic growth on the network while optimizing the use of existing resources—and delaying the need for further investments in equipment and services. That is, QoS enables you to:

- Specify which traffic has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.
- Override "illegal" packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. (Instead, control priority through network policy.)

QoS on the switches covered in this guide support these types of traffic marking:

- **802.1p prioritization:** Controls the outbound port queue priority for traffic leaving the switch, and (if traffic exits through a VLAN-tagged port) sends the priority setting with the individual packets to the downstream devices.
- **IP Type-of-Service (ToS):** Enables the switch to set, change, and honor prioritization policies by using the Differentiated Services (diffserv) bits in the ToS byte of IPv4 packet headers.

Terminology

Term	Use in This Document
802.1p priority	A traffic priority setting carried by a VLAN-tagged packet moving from one device to another through ports that are tagged members of the VLAN to which the packet belongs. This setting can be from 0 - 7. The switch handles an outbound packet on the basis of its 802.1p priority. However, if the packet leaves the switch through a VLAN on which the port is an untagged member, this priority is dropped, and the packet arrives at the next, downstream device without an 802.1p priority assignment.
802.1Q field	A four-byte field that is present in the header of Ethernet packets entering or leaving the switch through a port that is a tagged member of a VLAN. This field includes an 802.1p priority setting, a VLAN tag, or ID number (VID), and other data. A packet entering or leaving the switch through a port that is an untagged member of the outbound VLAN does not have this field in its header and thus does not carry a VID or an 802.1p priority. See also "802.1p priority".
codepoint	Refer to DSCP, below.
downstream device	A device linked directly or indirectly to an outbound switch port. That is, the switch sends traffic to downstream devices.
DSCP	***Differentiated Services Codepoint.*** (Also termed ***codepoint***.) A DSCP is comprised of the upper six bits of the ToS (Type-of-Service) byte in IP packets. There are 64 possible codepoints. In the default QoS configuration for the switches covered in this guide, some codepoints are configured with default 802.1p priority settings for Assured-Forwarding and Expedited Forwarding. All other codepoints are unused (and listed with **No-override** for a priority).
DSCP policy	A DSCP configured with a specific 802.1p priority (0- 7). (Default: **No-override**). Using a DSCP policy, you can configure the switch to assign priority to IP packets. That is, for an IP packet identified by the specified classifier, you can assign a new DSCP and an 802.1p priority (0-7). For more on DSCP, refer to "Details of QoS IP Type-of-Service" on page 5-24. For the DSCP map, see figure 5-10 on page 5-25.
edge switch	In the QoS context, this is a switch that receives traffic from the edge of the LAN or from outside the LAN and forwards it to devices within the LAN. Typically, an edge switch is used with QoS to recognize packets based on classifiers such as TCP/UDP application type, IP-device (address), Protocol (LAN), VLAN-ID (VID), and Source-Port (although it can also be used to recognize packets on the basis of ToS bits). Using this packet recognition, the edge switch can be used to set 802.1p priorities or DSCP policies that downstream devices will honor.
inbound port	Any port on the switch through which traffic enters the switch.
IP Options	In an IPv4 packet, optional, these are extra fields in the packet header.
IP-precedence bits	The upper three bits in the Type of Service (ToS) field of an IP packet.
IPv4	Version 4 of the IP protocol.
outbound packet	A packet leaving the switch through any LAN port.
outbound port	Any port on the switch through which traffic leaves the switch.

Term	Use in This Document
outbound port queue	For any port, a buffer that holds outbound traffic until it can leave the switch through that port. By default, there are eight outbound queues for each port in the switch. Queue 8 is the highest priority queue; queue 1 is the lowest priority queue. Traffic in a port's high priority queue leaves the switch before any traffic in the port's medium or low priority queues.
re-marking (DSCP re-marking)	Assigns a new QoS policy to an outbound packet by changing the DSCP bit settings in the ToS byte.
tagged port membership	Identifies a port as belonging to a specific VLAN and enables VLAN-tagged packets belonging to that VLAN to carry an 802.1p priority setting when outbound from that port. Where a port is an untagged member of a VLAN, outbound packets belonging to that VLAN do not carry an 802.1p priority setting.
Type-of-Service (ToS) byte	Comprised of a three-bit (high-order) precedence field and a five-bit (low-order) Type-of-Service field. Later implementations may use this byte as a six-bit (high-order) Differentiated Services field and a two-bit (low-order) reserved field. See also "IP-precedence bits" and DSCP elsewhere in this table.
upstream device	A device linked directly or indirectly to an inbound switch port. That is, the switch receives traffic from upstream devices.

Overview

QoS settings operate on two levels:

- **Controlling the priority of outbound packets moving through the switch:** Each switch port has four shared outbound traffic queues; the queue with a priority value of one has the lowest priority, and priority value four has the highest priority. Packets leave the switch port on the basis of their queue assignment and whether any higher queues are empty:

Table 5-1. Port Queue Exit Priorities

Port Queue and 802.1p Priority Values	Priority for Exiting From the Port
Low (1) Low (2)	Fourth
Normal (0) Normal (3)	Third
Medium (4) Medium (5)	Second
High (6) High (7)	First

A QoS configuration enables you to set the outbound priority queue to which a packet is sent. (In an 802.1Q VLAN environment with VLAN-tagged ports, if QoS is *not* configured on the switch, but *is* configured on an upstream device, the priorities carried in the packets determine the forwarding queues in the switch.)

- **Configuring a priority for outbound packets and a service (priority) policy for use by downstream devices:**
  - **DSCP Policy:** This feature enables you to set a priority policy in outbound IP packets. (You can configure downstream devices to read and use this policy.) This method is not dependent on VLAN-tagged ports to carry priority policy to downstream devices, and can:
    - Change the codepoint (the upper six bits) in the ToS byte.
    - Set a new 802.1p priority for the packet.

    (Setting DSCP policies requires IPv4 inbound packets. Refer to the "IPv4" entry under "Terminology" on page 5-6.)
  - **802.1p Priority Rules:** An outbound, VLAN-tagged packet carries an 802.1p priority setting that was configured (or preserved) in the switch. This priority setting ranges from 0 to 3, and can be used by downstream devices having up to four outbound port queues. Thus, while packets within the switch move at the four priority levels shown in table 5-1, above, they still can carry an 802.1p priority that can be used by downstream devices having more or less than the four priority levels in the switches covered in this guide. Also, if the packet enters the switch with an 802.1p priority setting, QoS can override this setting if configured with an 802.1p priority rule to do so.

Notes

If your network uses only one VLAN (and therefore does not require VLAN-tagged ports) you can still preserve 802.1p priority settings in your traffic by configuring the ports as tagged VLAN members on the links between devices you want to honor traffic priorities.

You can configure a QoS priority of 0 through 3 for an outbound packet. When the packet is then sent to a port, the QoS priority determines which outbound queue the packet uses:

Table 5-2. QoS Priority Settings and Operation

QoS Priority Setting	Outbound Port Queue
1-2	low priority (1,2)
0-3	normal priority (3,4)
4-5	medium priority (5,6)
6-7	high priority (7,8)

If a packet is not in a VLAN-tagged port environment, then the QoS settings in table 5-2 control only to which outbound queue the packet goes. Without VLAN tagging, no 802.1p priority is added to the packet for downstream device use. But if the packet is in a VLAN-tagged environment, then the above setting is also added to the packet as an 802.1p priority for use by downstream devices and applications (shown in table 5-3). In either case, an IP packet can also carry a priority policy to downstream devices by using DSCP-marking in the ToS byte.

Table 5-3. Mapping Switch QoS Priority Settings to Device Queues

Priority Setting	Outbound Port Queues in the Switch	802.1p Priority Setting Added to Tagged VLAN Packets Leaving the Switch	Queue Assignment in Downstream Devices With: 4 Queues
1	Queue 1	1 (low priority)	Queue 1
2		2	
0	Queue 2	0 (normal priority)	Queue 2
3		3	
4	Queue 3	4 (medium priority)	Queue 3
5		5	
6	Queue 4	6 (high priority)	Queue 4
7		7	

Note The number of outbound port queues in the switch is fixed at four.

Classifiers for Prioritizing Outbound Packets

Note On Using Multiple Criteria

ProCurve recommends that you configure a minimum number of the available QoS classifiers for prioritizing any given packet type. Increasing the number of active classifier options for a packet type increases the complexity of the possible outcomes and consumes switch resources.

Packet Classifiers and Evaluation Order

The switches covered in this guide provide the following QoS classifiers (packet criteria) you can use to configure QoS priority.

Table 5-4. Classifier Search Order and Precedence

Search Order	Precedence	QoS Classifier Type
1	1 (highest)	IP Type of Service (ToS) field (IP packets only)
2	2	Incoming source-port on the switch
3	3 (lowest)	Incoming 802.1p Priority (present in tagged VLAN environments)

Where multiple classifier types are configured, a switch uses the highest-to-lowest search order shown in table 5-4 to identify the highest-precedence classifier to apply to any given packet. When a match between a packet and a classifier is found, the switch applies the QoS policy configured for that classifier and the packet is handled accordingly.

Note that on the switches covered in this guide, if the switch is configured with multiple classifiers that address the same packet, the switch uses only the QoS configuration for the QoS classifier that has the highest precedence. In this case, the QoS configuration for another, lower-precedence classifier that may apply is ignored.

Preparation for Configuring QoS

Preserving 802.1p Priority

QoS operates in VLAN-tagged and VLAN-untagged environments. If your network does not use multiple VLANs, you can still implement the 802.1Q VLAN capability for packets to carry their 802.1p priority to the next downstream device. To do so, configure ports as VLAN-tagged members on the links between switches and routers in your network infrastructure.

Table 5-5. Summary of QoS Capabilities

Outbound Packet Options	Port Membership in VLANs	
	Tagged	Untagged
Control Port Queue Priority for Packet Types	Yes	Yes
Carry 802.1p Priority Assignment to Next Downstream Device	Yes	No
Carry DSCP Policy to Downstream Devices. The policy includes:	Yes[1]	Yes[1]
Assigning a ToS Codepoint		
Assigning an 802.1p Priority [2] to the Codepoint		

[1] Except for non-IPv4 packets or packets processed using either the Layer 3 Protocol or QoS IP-Precedence methods, which do not include the DSCP policy option. Also, to use a service policy in this manner, the downstream devices must be configured to interpret and use the DSCP carried in the IP packets.

[2] This priority corresponds to the 802.1p priority scheme and is used to determine the packet's port queue priority. When used in a VLAN-tagged environment, this priority is also assigned as the 802.1p priority carried outbound in packets having an 802.1Q field in the header.

Steps for Configuring QoS on the Switch

1. Determine the QoS policy you want to implement. This includes analyzing the types of traffic flowing through your network and identifying one or more traffic types to prioritize. In order of QoS precedence, these are:
   a. IP Type-of-Service Precedence Bits (Leftmost three bits in the ToS field of IP packets)
   b. IP Type-of-Service Differentiated Service bits (Leftmost six bits in the ToS field of IP packets)
   c. Source-Port
   d. Incoming 802.1p Priority (requires at least one tagged VLAN on the network)

2. Select the QoS option you want to use. Table 5-6 lists the traffic types (QoS classifiers) and the QoS options you can use for prioritizing or setting a policy on these traffic types:

Table 5-6. Applying QoS Options to Traffic Types Defined by QoS Classifiers

QoS Options for Prioritizing Outbound Traffic		QoS Classifiers		
		IP-ToS Precedence	IP-DiffServ	Source-Port
Option 1: Configure80 2.1p Priority Rules Only	Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch. Rely on VLAN-tagged ports to carry packet priority as an 802.1p value to downstream devices.	Yes[1]	Yes	Yes
Option 2: Configure ToS DSCP Policies with 802.1p Priorities	Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch. Propagate a service policy by reconfiguring the DSCP in outbound IP packets according to packet type. The packet is placed in an outbound port queue according to the 802.1p priority configured for that DSCP policy. (The policy assumes that downstream devices can be configured to recognize the DSCP in IP packets and implement the service policy it indicates.) Use VLAN-tagged ports to include packet priority as an 802.1p value to downstream devices.	No	Yes	Yes

[1] In this mode the configuration is fixed. You cannot change the automatic priority assignment when using IP-ToS Precedence as a QoS classifier.

3. If you want 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate downstream links.

4. Determine the actual QoS configuration changes you will need to make on each QoS-capable device in your network in order to implement the desired policy. Also, if you want downstream devices to read and use DSCPs in IP packets from the switch, configure them to do so by enabling ToS Differentiated Service mode and making sure the same DSCP policies are configured.

Viewing the QoS Configuration

The following show commands are available on the switches covered in this guide. Examples of the **show qos** output are included with the example for each priority type.

Syntax: show qos < *priority-classifier* >

dscp-map

Show mappings between DSCP policy and 802.1p priority.

port-priority

Displays the current source-port priority configuration. Refer to figure 5-11 on page 5-28.

type-of-service

Displays the current type-of-service priority configuration. The display output differs according to the ToS option used:

- *IP Precedence: Refer to figure 5-3 on page 5-16.*
- *Diffserve: Refer to figure 5-5 on page 5-19.*

No Override

By default, the IP ToS, Protocol, and (source) port **show** outputs automatically list **No-override** for priority options that have not been configured. This means that if you do not configure a priority for a specific option, QoS does not prioritize packets to which that option applies, resulting in the **No override** state. In this case, IP packets received through a VLAN-tagged port receive whatever 802.1p priority they carry in the 802.1Q tag in the packet's header. VLAN-Tagged packets received through an untagged port are handled in the switch with "normal" priority.

Using QoS Classifiers to Configure Quality of Service for Outbound Traffic

QoS Feature	Default	Reference
IP Type-of-Service Priority	Disabled	page 5-15
Source-Port Priority	Disabled	page 5-27

Note In addition to the information in this section on the various QoS classifiers, refer to "QoS Operating Notes and Restrictions" on page 5-41.

QoS IP Type-of-Service (ToS) Policy and Priority

QoS Classifier Precedence: 1

This feature applies only to IPv4 traffic and performs either of the following:

- **ToS IP-Precedence Mode:** All IP packets generated by upstream devices and applications include precedence bits in the ToS byte. Using this mode, the switch uses these bits to compute and assign the corresponding 802.1p priority.
- **ToS Differentiated Services (Diffserv) Mode:** This mode requires knowledge of the codepoints set in IP packets by the upstream devices and applications. It uses the ToS codepoint in IP packets coming from upstream devices and applications to assign 802.1p priorities to the packets. You can use this option to do both of the following:
  - **Assign a New Prioritization Policy:** A "policy" includes both a codepoint and a corresponding 802.1p priority. This option selects an incoming IPv4 packet on the basis of its codepoint and assigns a new codepoint and corresponding 802.1p priority. (Use the **qos dscp-map** command to specify a priority for any codepoint—page 5-33.)
  - **Assign an 802.1p Priority:** This option reads the DSCP of an incoming IPv4 packet and, without changing this codepoint, assigns the 802.1p priority to the packet, as configured in the DSCP Policy Table (page 5-33). This means that a priority value of 0 - 7 must be configured for a DSCP before the switch will attempt to perform a QoS match on the packet's DSCP bits.

  Before configuring the ToS Diffserv mode, you must use the **dscp-map** command to configure the desired 802.1p priorities for the codepoints you want to use for either option. This command is illustrated in the following examples and is described under "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.

Unless IP-Precedence mode and Diffserv mode are both disabled (the default setting), enabling one automatically disables the other. For more on ToS operation, refer to "Details of QoS IP Type-of-Service" on page 5-24.

Assigning an 802.1p Priority to IPv4 Packets on the Basis of the ToS Precedence Bits

If a device or application upstream of the switch sets the precedence bits in the ToS byte of IPv4 packets, you can use this feature to apply that setting for prioritizing packets for outbound port queues. If the outbound packets are in a tagged VLAN, this priority is carried as an 802.1p value to the adjacent downstream devices.

Syntax: qos type-of-service ip-precedence

Causes the switch to automatically assign an 802.1p priority to all IPv4 packets by computing each packet's 802.1p priority from the precedence bits the packet carries. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. (ToS IP Precedence Default: Disabled)

no qos type-of-service

Disables all ToS classifier operation, including prioritization using the precedence bits.

show qos type-of-service

When ip-precedence is enabled (or if neither ToS option is configured), shows the ToS configuration status. If diff-services is enabled, lists codepoint data as described under "Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices" on page 5-21.

With this option, prioritization of outbound packets relies on the IP-Precedence bit setting that IP packets carry with them from upstream devices and applications. To configure and verify this option:

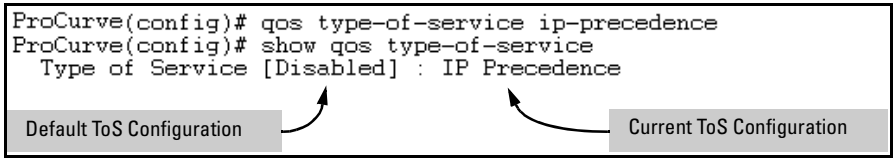

ProCurve(config)# qos type-of-service ip-precedence
ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : IP Precedence
Default ToS Configuration
Current ToS Configuration

Figure 5-3. Example of Enabling ToS IP-Precedence Prioritization

To replace this option with the ToS diff-services option, configure **diff-services** as described below, which automatically disables IP-Precedence. To disable IP-Precedence without enabling the diff-services option, use this command:

```
ProCurve(config)# no qos type-of-service
```

Assigning an 802.1p Priority to IPv4 Packets on the Basis of Incoming DSCP

One of the best uses for this option is on an interior switch where you want to honor (continue) a policy set on an edge switch. That is, it enables you to select incoming packets having a specific DSCP and forward these packets with the desired 802.1p priority. For example, if an edge switch "A" marks all packets received on port A5 with a particular DSCP, you can configure a downstream (interior) switch "B" to handle such packets with the desired priority (regardless of whether 802.1Q tagged VLANs are in use).

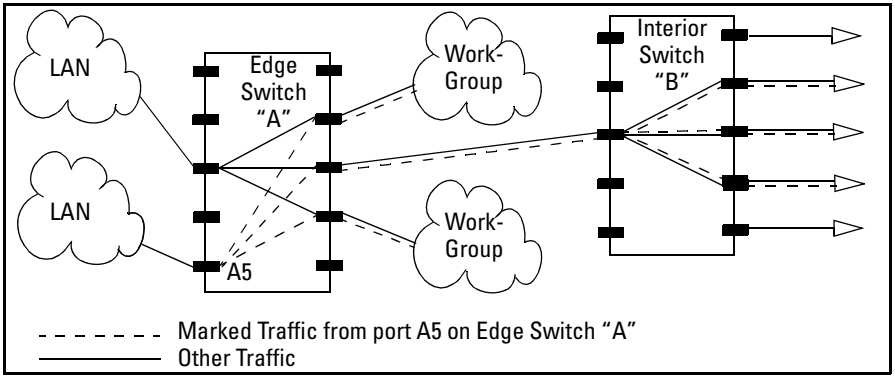


Figure 5-4. Interior Switch "B" Honors the Policy Established in Edge Switch "A"

To do so, assign the desired 802.1p priority to the same codepoint that the upstream or edge switch assigns to the selected packets. When the downstream switch receives an IPv4 packet carrying one of these codepoints, it assigns the configured priority to the packet and sends it out the appropriate priority queue. (The packet retains the codepoint it received from the upstream or edge switch). You can use this option concurrently with the diffserv DSCP Policy option (described later in this section), as long as the DSCPs specified in the two options do not match.

Operating Notes

Different applications may use the same DSCP in their IP packets. Also, the same application may use multiple DSCPs if the application originates on different clients, servers, or other devices. Using an edge switch enables you to select the packets you want and mark them with predictable DSCPs that can be used by downstream switches to honor policies set in the edge switch.

When enabled, the switch applies direct 802.1p prioritization to all packets having codepoints that meet these criteria:

- The codepoint is configured with an 802.1p priority in the DSCP table. (Codepoints configured with **No-override** are not used.)
- The codepoint is not configured for a new DSCP policy assignment.

Thus, the switch does not allow the same incoming codepoint (DSCP) to be used simultaneously for directly assigning an 802.1p priority and also assigning a DSCP policy. For a given incoming codepoint, if you configure one option and then the other, the second overwrites the first.

To use this option:

1. Identify a DSCP used to set a policy in packets received from an upstream or edge switch.
2. Determine the 802.1p priority (0 - 7) you want to apply to packets carrying the identified DSCP. (You can either maintain the priority assigned in the upstream or edge switch, or assign a new priority.)
3. Use **qos dscp-map < *codepoint* > priority < 0 - 7 >** to assign the 802.1p priority you want to the specified DSCP. (For more on this topic, refer to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.)
4. Enable **diff-services**.

Syntax: qos type-of-service diff-services < *codepoint* >

Causes the switch to read the **< *codepoint* >** *(DSCP) of an incoming IPv4 packet and, when a match occurs, assign a corresponding 802.1p priority, as configured in the switch's DSCP table (page 5-34).*

no qos type-of-service

Disables all ToS classifier operation.

no qos dscp-map < *codepoint* >

Disables direct 802.1p priority assignment to packets carrying the < ***codepoint*** *> by reconfiguring the codepoint priority assignment in the DSCP table to* **No-override**. *Note that if this codepoint is in use as a DSCP policy for another diffserv codepoint, you must disable or redirect the other diffserv codepoint's DSCP policy before you can disable or change the codepoint. For example, in figure 5-5 you cannot change the priority for the 000000 codepoint until you redirect the DSCP policy for 000001 away from using 000000 as a policy. (Refer to "Notes on Changing a Priority Setting" on page 5-36. Refer also to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.)*

show qos type-of-service

Displays current Type-of-Service configuration. In diffserv mode it also shows the current direct 802.1p assignments and the current DSCP assignments covered later in this section.

For example, an edge switch "A" in an untagged VLAN assigns a DSCP of 000110 on IP packets it receives on port A6, and handles the packets with high priority (7). When these packets reach interior switch "B" you want the switch to handle them with the same high priority. To enable this operation you would configure an 802.1p priority of 7 for packets received with a DSCP of **000110**, and then enable **diff-services**:

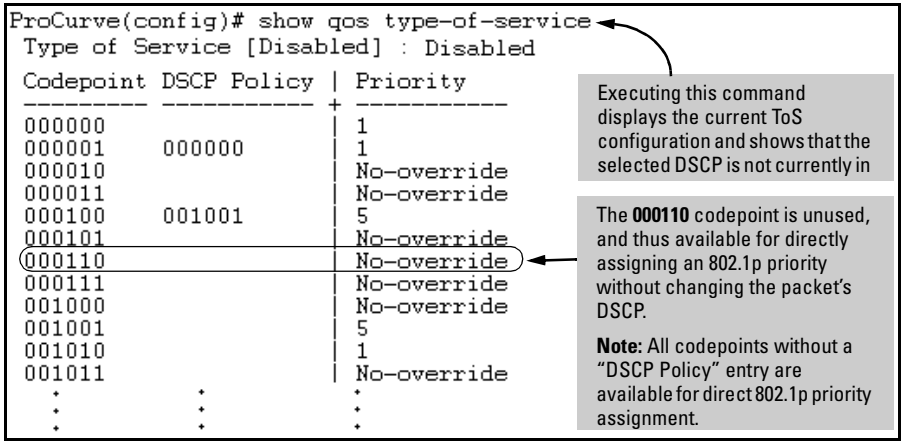

ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : Disabled
Codepoint DSCP Policy | Priority
000000 | 1
000001 000000 | 1
000010 | No-override
000011 | No-override
000100 001001 | 5
000101 | No-override
000110 | No-override
000111 | No-override
001000 | No-override
001001 | 5
001010 | 1
001011 | No-override
Executing this command displays the current ToS configuration and shows that the selected DSCP is not currently in
The 000110 codepoint is unused, and thus available for directly assigning an 802.1p priority without changing the packet's DSCP.
Note: All codepoints without a "DSCP Policy" entry are available for direct 802.1p priority assignment.

Figure 5-5. Example Showing Codepoints Available for Direct 802.1p Priority Assignments

```
ProCurve(config)# qos dscp-map 000110 priority 7
ProCurve(config)# qos type-of-service diff-services

ProCurve(config)# show qos type-of-service
  Type of Service [Disabled] : Differentiated Services
  Codepoint DSCP Policy | Priority
  --------- ----------- + -----------
  000000                | 1
  000001    000000      | 1
  000010                | No-override
  000011                | No-override
  000100    001001      | 5
  000101                | No-override
  000110                | 7
  000111                | No-override
  001000                | No-override
  001001                | 5
     .          .         .
     .          .         .
     .          .         .
```

Outbound IP packets with a DSCP of **000110** will have a priority of **7**.

Notice that codepoints **000000** and **001001** are named as DSCP policies by other codepoints (**000001** and **000110** respectively). This means they are not available for changing to a different 802.1p priority.

Figure 5-6. Example of a Type-of-Service Configuration Enabling Both Direct 802.1p Priority Assignment and DSCP Policy Assignment

Assigning a DSCP Policy on the Basis of the DSCP in IPv4 Packets Received from Upstream Devices

The preceding section describes how to forward a policy set by an edge (or upstream) switch. This option changes a DSCP policy in an IPv4 packet by changing its IP ToS codepoint and applying the priority associated with the new codepoint. (A DSCP policy consists of a differentiated services codepoint and an associated 802.1p priority.) You can use this option concurrently with the diffserv 802.1p priority option (above), as long as the DSCPs specified in the two options do not match.

To use this option to configure a change in policy:

1. Identify a DSCP used to set a policy in packets received from an upstream or edge switch.
2. Create a new policy by using **qos dscp-map < *codepoint* > priority < 0 - 7 >** to configure an 802.1p priority for the codepoint you will use to overwrite the DSCP the packet carries from upstream. (For more on this topic, refer to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.)
3. Use **qos type-of-service diff-services < *incoming-DSCP* > dscp < *outgoing-DSCP* >** to change the policy on packets coming from the edge or upstream switch with the specified incoming DSCP.

   (Figure 5-4 on page 5-17 illustrates this scenario.)

Note

On the switches covered in this guide, DSCP policies (codepoint re-marking) cannot be applied to outbound IPv4 packets having IP options. (The 802.1p priority in the VLAN tag is applied.) For more information on packet criteria and restrictions, refer to table 5-11 on page 5-41.

Syntax: qos type-of-service diff-services

Enables ToS diff-services.

Syntax: qos type-of-service diff-services < *current-codepoint* > dscp < *new-codepoint* >

Configures the switch to select an incoming IP packet carrying the <***current-codepoint***> *and then use the* <***new-codepoint***> *to assign a new, previously configured DSCP policy to the packet. The policy overwrites the* <***current-codepoint***> *with the* < ***new-codepoint***> *and assigns the 802.1p priority specified by the policy. (Use the* **qos dscp-map** *command to define the priority for the DSCPs—page 5-33.)*

Syntax: no qos type-of-service

Disables all ToS classifier operation. Current ToS DSCP policies and priorities remain in the configuration and will become available if you re-enable ToS diff-services.

Syntax: no qos type-of-service [diff-services < *codepoint* >]

Deletes the DSCP policy assigned to the < ***codepoint*** > *and returns the* < ***codepoint*** > *to the 802.1p priority setting it had before the DSCP policy was assigned. (This will be either a value from 0 - 7 or* **No-override***.)*

Syntax: show qos type-of-service

Displays a listing of codepoints, with any corresponding DSCP policy re-assignments for outbound packets. Also lists the (802.1p) priority for each codepoint that does not have a DSCP policy assigned to it.

For example, suppose you want to configure the following two DSCP policies for packets received with the indicated DSCPs.

Received DSCP	Policy DSCP	802.1p Priority	Policy Name (Optional)
001100	000010	6	Level 6
001101	000101	4	Level 4

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Notes on Changing a Priority Setting” on page 5-36. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

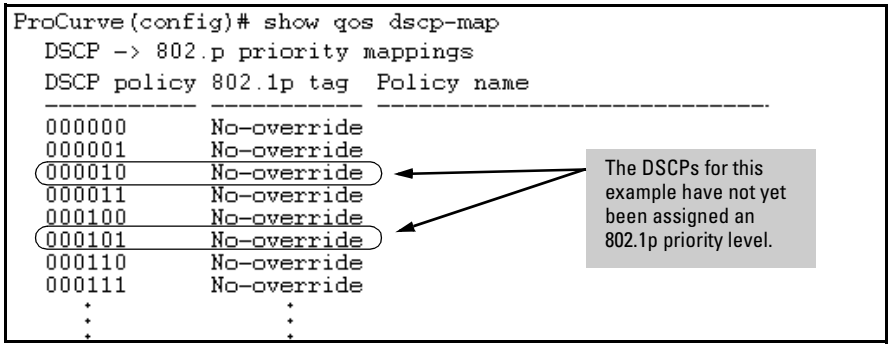


Figure 5-7. Display the Current DSCP-Map Configuration

2. Configure the policies in the DSCP table:

```
ProCurve(config)# qos dscp-map 000010 priority 6 name 'Level 6'
ProCurve(config)# qos dscp-map 000101 priority 4 name 'Level 4'

ProCurve(config)# show qos dscp-map
  DSCP -> 802.p priority mappings
  DSCP policy 802.1p tag  Policy name
  ----------- ----------- --------------------------------
  000000      No-override
  000001      No-override
  000010      6           Level 6
  000011      No-override
  000100      No-override
  000101      4           Level 4
  000110      No-override
  000111      No-override
     .           .           .
     .           .           .
     .           .           .
```

Figure 5-8. Example of Policies Configured (with Optional Names) in the DSCP Table

3. Assign the policies to the codepoints in the selected packet types.

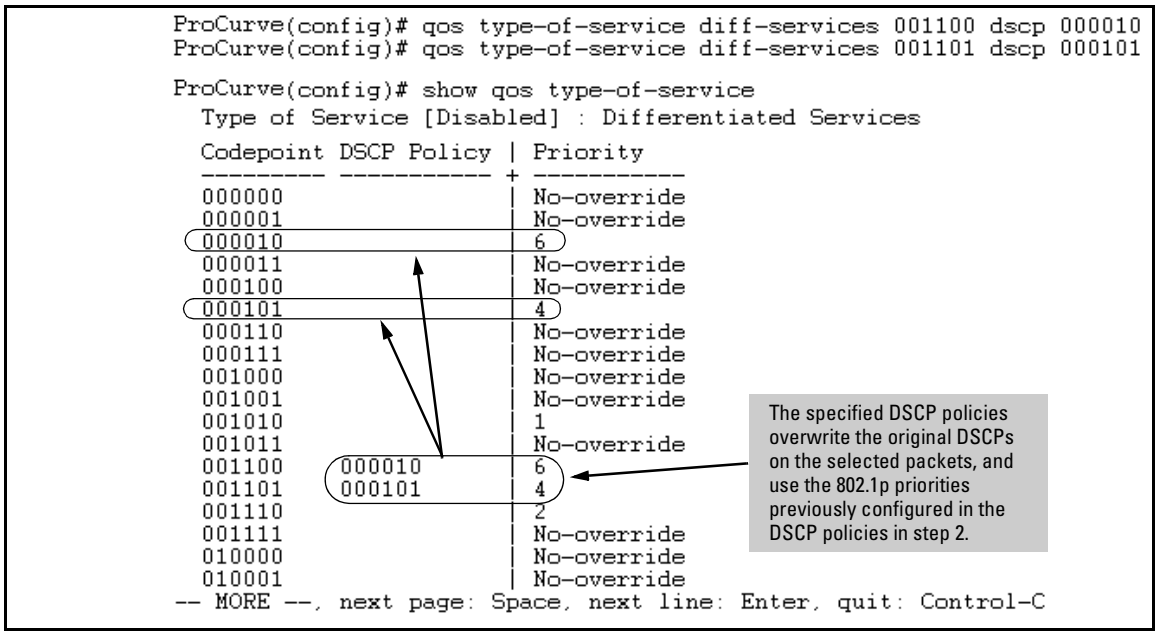

ProCurve(config)# qos type-of-service diff-services 001100 dscp 000010
ProCurve(config)# qos type-of-service diff-services 001101 dscp 000101
ProCurve(config)# show qos type-of-service
Type of Service [Disabled] : Differentiated Services
Codepoint DSCP Policy | Priority
000000 | No-override
000001 | No-override
000010 | 6
000011 | No-override
000100 | No-override
000101 | 4
000110 | No-override
000111 | No-override
001000 | No-override
001001 | No-override
001010 | 1
001011 | No-override
001100 000010 | 6
001101 000101 | 4
001110 | 2
001111 | No-override
010000 | No-override
010001 | No-override
-- MORE --, next page: Space, next line: Enter, quit: Control-C
The specified DSCP policies overwrite the original DSCPs on the selected packets, and use the 802.1p priorities previously configured in the DSCP policies in step 2.

Figure 5-9. Example of Policy Assignment to Outbound Packets on the Basis of the DSCP in the Packets Received from Upstream Devices

Details of QoS IP Type-of-Service

IP packets include a Type of Service (ToS) byte. The ToS byte includes:

- **A Differentiated Services Codepoint (DSCP):** This element is comprised of the upper six bits of the ToS byte). There are 64 possible codepoints.
  - In the switches covered in this guide, the default **qos** configuration includes some codepoints with 802.1p priority settings for Assured-Forwarding and Expedited Forwarding (codepoint 101110), while others are unused (and listed with **No-override** for a Priority).

  Refer to figure 5-9 on page 5-34 for an illustration of the default DSCP policy table.

  Using the **qos dscp map** command, you can configure the switch to assign different prioritization policies to IPv4 packets having different codepoints. As an alternative, you can configure the switch to assign a new codepoint to an IPv4 packet, along with a corresponding 802.1p priority (0-7). To use this option in the simplest case, you would:

a. Configure a specific DSCP with a specific priority in an edge switch.

b. Configure the switch to mark a specific type of inbound traffic with that DSCP (and thus create a policy for that traffic type).

c. Configure the internal switches in your LAN to honor the policy.

(For example, you could configure an edge switch to assign a codepoint of 000001 to all packets received from a specific VLAN, and then handle all traffic with that codepoint at high priority.)

For a codepoint listing and the commands for displaying and changing the DSCP Policy table, refer to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.

- **Precedence Bits:** This element is a subset of the DSCP and is comprised of the upper three bits of the ToS byte. When configured to do so, the switch uses the precedence bits to determine a priority for handling the associated packet. (The switch does not change the setting of the precedence bits.) Using the ToS Precedence bits to prioritize IPv4 packets relies on priorities set in upstream devices and applications.

Figure 5-10 shows an example of the ToS byte in the header for an IPv4 packet, and illustrates the diffserv bits and precedence bits in the ToS byte. (Note that the Precedence bits are a subset of the Differentiated Services bits.)

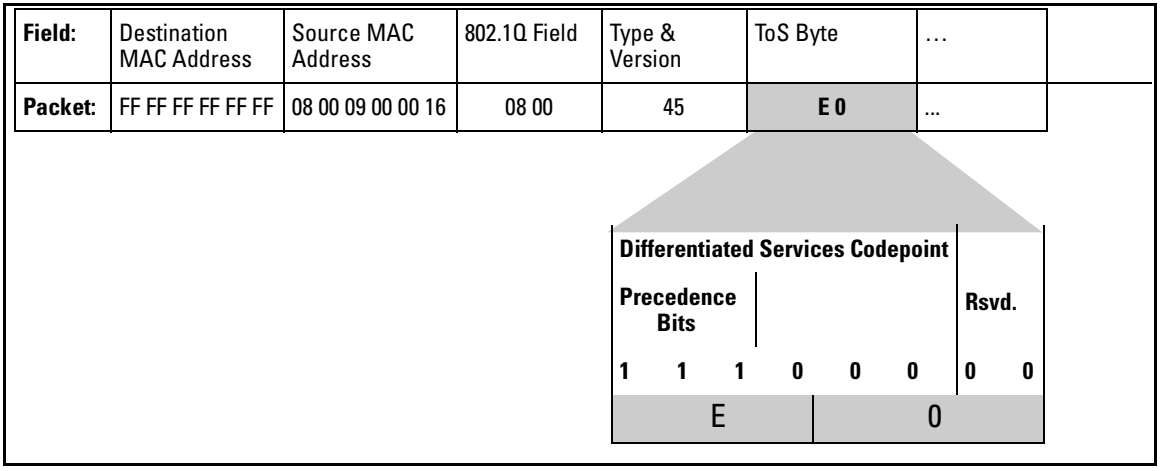


Figure 5-10. The ToS Codepoint and Precedence Bits

Table 5-7. How the Switch Uses the ToS Configuration

Outbound Port	ToS Option:	
	802.1p (Value = 0 - 7)	Differentiated Services
IP Packet Sent Out an Untagged Port in a VLAN	Depending on the value of the IP Precedence bits in the packet's ToS field, the packet will go to one of four outbound port queues in the switch: 1-2 = low priority (queue 1) 0-3 = normal priority (queue 2) 4-5 = medium priority (queue 3) 6-7 = high priority (queue 4)	For a given packet carrying a ToS codepoint that the switch has been configured to detect: • Change the codepoint according to the configured policy and assign the 802.1p priority specified for the new codepoint in the DSCP Policy Table (page 5-33). • Do not change the codepoint, but assign the 802.1p priority specified for the existing codepoint in the DSCP Policy Table (page 5-33). Depending on the 802.1p priority used, the packet will leave the switch through one of the following queues: 1 - 2 = low priority (queue 1) 0 - 3 = normal priority (queue 2) 4 - 5 = medium priority (queue 3) 6 - 7 = high priority (queue 4) If **No-override** (the default) has been configured for a specified codepoint, then the packet is not prioritized by ToS and, by default, is sent to the "normal priority" queue.
IP Packet Sent Out an Untagged Port in a VLAN	Same as above, plus the IP Precedence value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device. Refer to table 5-8, below.	Same as above, plus the Priority value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device. Where **No-override** is the assigned priority, the VLAN tag carries a "0" (normal priority) 802.1p setting if not prioritized by other QoS classifiers.

Table 5-8. ToS IP-Precedence Bit Mappings to 802.1p Priorities

ToS Byte IP Precedence Bits	Corresponding 802.1p Priority	Service Priority Level
000	1	Lowest
001	2	Low
002	0	Normal
003	3	
004	4	
005	5	
006	6	
007	7	Highest

QoS Source-Port Priority

QoS Classifier Precedence: 2

The QoS source-port option enables you to use a packet's source-port on the switch as a QoS classifier. Where a particular source-port classifier has the highest precedence in the switch for traffic entering through that port, then traffic received from the port is marked with the source-port classifier's configured priority level. Different source-port classifiers can have different priority levels.

Options for Assigning Priority on the Switch. Priority control options for packets from a specified source-port include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to "Classifiers for Prioritizing Outbound Packets" on page 5-10.)

Options for Assigning Priority From a RADIUS Server. You can use a RADIUS server to impose a QoS source-port priority during an 802.1X port-access authentication session. Refer to the RADIUS chapter in the *Access Security Guide* for your switch.

Assigning a Priority Based on Source-Port

This option assigns a priority to all outbound packets having the specified source-port. You can configure this option by either specifying the source-port ahead of the **qos** command or moving to the port context for the port you want to configure for priority. (If you are configuring multiple source-ports with the same priority, you may find it easier to use the **interface < *port-list* >** command to go to the port context instead of individually configuring the priority for each port.)

Syntax: interface < *port-list* > qos priority < 0 - 7 >

Configures an 802.1p priority for packets entering the switch through the specified (source) ports. This priority determines the packet queue in the outbound port(s) to which traffic is sent. If a packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each source-port or group of source-ports. (Default: **No-override***)*

Syntax: no interface < *port-list* > qos

Disables use of the specified source-port(s) for QoS classifier(s) and resets the priority for the specified source-port(s) to **No-override**.

Syntax: show qos port-priority

Lists the QoS port-priority classifiers with their priority data.

For example, suppose that you want to prioritize inbound traffic on the following source-ports:

Source-Port	Priority
A1 - A3	2
A4	3
B1, B4	5
C1-C3	6

You would then execute the following commands to prioritize traffic received on the above ports:

```
ProCurve(config)# interface e c1-c3 qos priority 6
ProCurve(config)# interface e b1,b4 qos priority 5
ProCurve(config)# interface e a4 qos priority 3
ProCurve(config)# interface e a1-a3 qos priority 2

ProCurve(config)# show qos port-priority
  Port priorities
  Port  Apply rule   | DSCP   Priority    Radius Override
  ----  -----------  + ------ ----------- ---------------
  A1    Priority     |        2           No-override
  A2    Priority     |        2           No-override
  A3    Priority     |        2           No-override
  A4    Priority     |        3           No-override
  B1    Priority     |        5           No-override
  B2    No-override  |        No-override No-override
  B3    No-override  |        No-override No-override
  B4    Priority     |        5           No-override
  C1    Priority     |        6           No-override
  C2    Priority     |        6           No-override
  C3    Priority     |        6           No-override
  C4    No-override  |        No-override No-override
  C5    No-override  |        No-override No-override
   .         .                   .
   .         .                   .
   .         .                   .
```

Figure 5-11. Configuring and Displaying Source-Port QoS Priorities

If you then decided to remove port A1 from QoS prioritization:

```
ProCurve(config)# no interface e a1 qos
ProCurve(config)# show qos port-priority
  Port priorities

  Port Apply rule   | DSCP   Priority     Radius Override
  ---- ------------ + ------ ------------ ---------------
  A1   No-override  |        No-override  No-override
  A2   Priority     |        2            No-override
  A3   Priority     |        2            No-override
  A4   Priority     |        3            No-override
```

In this instance, **No-override** indicates that port A1 is not prioritized by QoS.

Figure 5-12. Returning a QoS-Prioritized VLAN to "No-override" Status

Assigning a DSCP Policy Based on the Source-Port

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets (received from the specified source-ports). That is, the switch:

1. Selects an incoming IP packet on the basis of its source-port on the switch.
2. Overwrites the packet's DSCP with the DSCP configured in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to "Terminology" on page 5-6.

Steps for Creating a Policy Based on Source-Port Classifiers.

Note

You can select one DSCP per source-port. Also, configuring a new DSCP for a source-port automatically overwrites (replaces) any previous DSCP or 802.1p priority configuration for that port.)

1. Identify the source-port classifier to which you want to assign a DSCP policy.
2. Determine the DSCP policy for packets having the selected source-port:
   a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received through the source-port from upstream devices.)
   b. Determine the 802.1p priority you want to assign to the DSCP.

3. Configure the DSCP policy by using **qos dscp-map** to configure the priority for each codepoint. (For details, refer to the example later in this section and to "Differentiated Services Codepoint (DSCP) Mapping" on page 5-33.)

Note

A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure that codepoint as a criteria for prioritizing packets by source-port. If a codepoint shows **No-override** in the **Priority** column of the DSCP Policy Table (**show qos dscp-map**), then you must assign a 0 - 7 priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets from the specified source-port.

Syntax: qos dscp-map < *codepoint* > priority < 0 - 7 >

This command is optional if a priority has already been assigned to the < ***codepoint*** >*. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this priority to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. (Default: For most codepoints,* **No-override**. *See figure 5-9 on page 5-34 on page 5-34.)*

Syntax: interface < *port-list* > qos dscp < *codepoint* >

Assigns a DSCP policy to packets from the specified source-port(s), and overwrites the DSCP in these packets with the assigned < ***codepoint*** > *value. This policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch on a tagged port, it carries the 802.1p priority with it to the next downstream device. (Default:* **No-override***)*

Syntax: no interface [e] < *port-list* > qos

Removes QoS classifier for the specified source-port(s).

Syntax: show qos source-port

Displays a listing of all source-port QoS classifiers currently in the running-config file.

For example, suppose you wanted to assign this set of priorities:

Source-Port	DSCP	Priority
A2	000111	7
B1-B3	000101	5
B4, C2	000010	1

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the "Notes on Changing a Priority Setting" on page 5-36. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

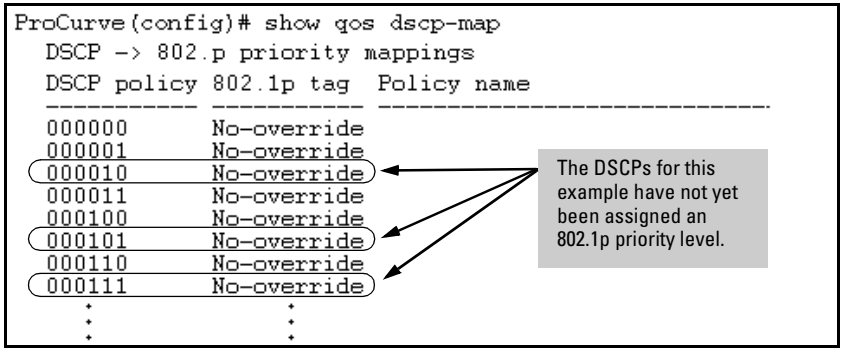


Figure 5-13. Display the Current Configuration in the DSCP Policy Table

2. Configure the priorities for the DSCPs you want to use.

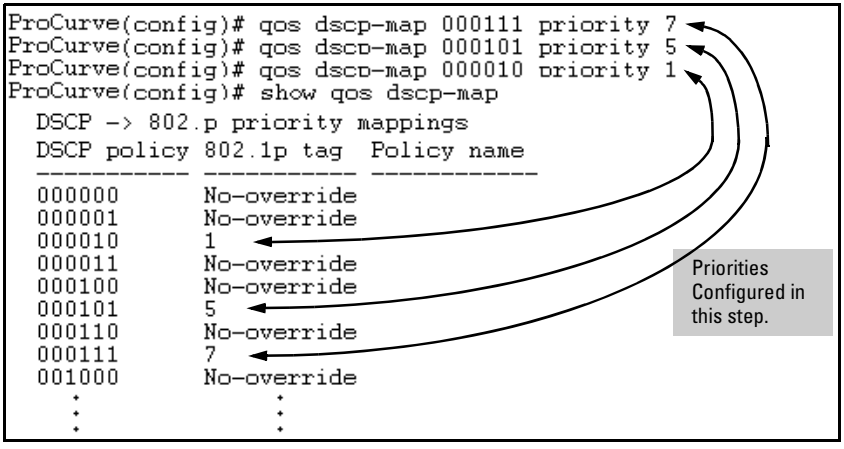


Figure 5-14. Assign Priorities to the Selected DSCPs

3. Assign the DSCP policies to the selected source-ports and display the result.

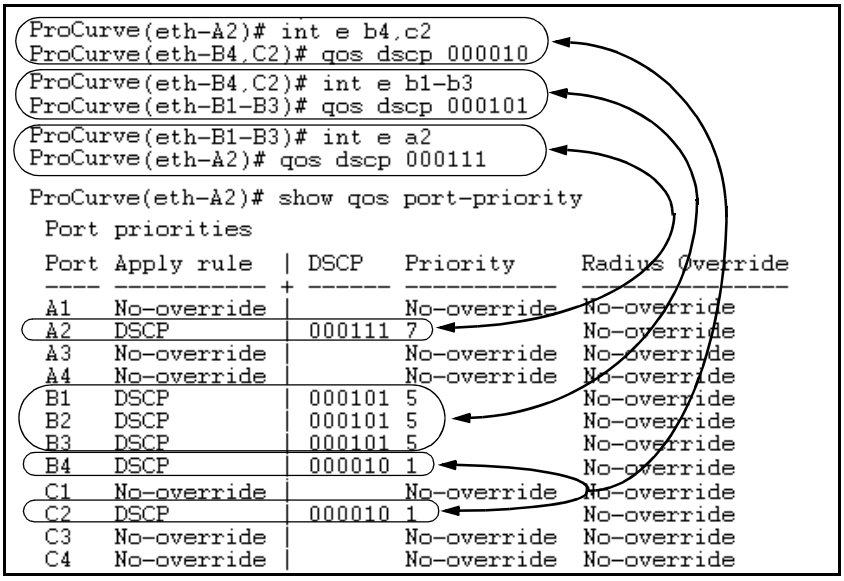

ProCurve(eth-A2)# int e b4,c2
ProCurve(eth-B4,C2)# qos dscp 000010
ProCurve(eth-B4,C2)# int e b1-b3
ProCurve(eth-B1-B3)# qos dscp 000101
ProCurve(eth-B1-B3)# int e a2
ProCurve(eth-A2)# qos dscp 000111
ProCurve(eth-A2)# show qos port-priority
Port priorities
Port Apply rule | DSCP Priority Radius Override
A1 No-override | No-override No-override
A2 DSCP | 000111 7 No-override
A3 No-override | No-override No-override
A4 No-override | No-override No-override
B1 DSCP | 000101 5 No-override
B2 DSCP | 000101 5 No-override
B3 DSCP | 000101 5 No-override
B4 DSCP | 000010 1 No-override
C1 No-override | No-override No-override
C2 DSCP | 000010 1 No-override
C3 No-override | No-override No-override
C4 No-override | No-override No-override

Figure 5-15. The Completed Source-Port DSCP-Priority Configuration

Radius Override Field. During a client session authenticated by a RADIUS server, the server can impose a port priority that applies only to that client session. Refer to the RADIUS chapter in the *Access Security Guide* for your switch.

Differentiated Services Codepoint (DSCP) Mapping

The DSCP Policy Table associates an 802.1p priority with a specific ToS byte codepoint in an IPv4 packet. This enables you to set a LAN policy that operates independently of 802.1Q VLAN-tagging.

In the default state, most of the 64 codepoints do not assign an 802.1p priority, as indicated by **No-override** in table 5-9 on page 5-34.

You can use the following command to list the current DSCP Policy table, change the codepoint priority assignments, and assign optional names to the codepoints.

Syntax: show qos dscp-map

Displays the DSCP Policy Table.

qos dscp-map **< *codepoint* >** priority < 0 - 7 > [name **< *ascii-string* >**]

Configures an 802.1p priority for the specified codepoint and, optionally, an identifying (policy) name.

no qos dscp-map **< *codepoint* >**

Reconfigures the 802.1p priority for <***codepoint***> *to* **No-override**. *Also deletes the codepoint policy name, if configured.*

no qos dscp-map < *codepoint* > name

Deletes only the ***policy name, if*** *configured, for* < ***codepoint*** >.

Table 5-9. The Default DSCP Policy Table

DSCP Policy	802.1p Priority	DSCP Policy	802.1p Priority	DSCP Policy	802.1p Priority
000000	No-override	010110	3*	101011	No-override
000001	No-override	010111	No-override	101100	No-override
000010	No-override	011000	No-override	101101	No-override
000011	No-override	011001	No-override	101110	7**
000100	No-override	011010	4*	101111	No-override
000101	No-override	011011	No-override	110000	No-override
000110	No-override	011100	4*	110001	No-override
000111	No-override	011101	No-override	110010	No-override
001000	No-override	011110	5*	110011	No-override
001001	No-override	011111	No-override	110100	No-override
001010	1*	100000	No-override	110101	No-override
001011	No-override	100001	No-override	110110	No-override
001100	1*	100010	6*	110111	No-override
001101	No-override	100011	No-override	111000	No-override
001110	2*	100100	6*	111001	No-override
001111	No-override	100101	No-override	111010	No-override
010000	No-override	100110	7*	111011	No-override
010001	No-override	100111	No-override	111100	No-override
010010	0 *	101000	No-override	111101	No-override
010011	No-override	101001	No-override	111110	No-override
010100	0 *	101010	No-override	111111	No-override
010101	No-override				

*Assured Forwarding codepoints; configured by default on the switches covered in this guide. These codepoints are configured as "No-override".

**Expedited Forwarding codepoint configured by default.

Default Priority Settings for Selected Codepoints

In a few cases, such as 001010 and 001100, a default policy (implied by the DSCP standards for Assured-Forwarding and Expedited-Forwarding) is used. You can change the priorities for the default policies by using **qos dscp-map < *codepoint*> priority < 0 - 7 >)**.(These policies are not in effect unless you have either applied the policies to a QoS classifier or configured QoS Type-of-Service to be in **diff-services** mode.)

Quickly Listing Non-Default Codepoint Settings

Table 5-9 lists the switch's default codepoint/priority settings. If you change the priority of any codepoint setting to a non-default value and then execute **write memory**, the switch will list the non-default setting in the show config display.

For example, in the default configuration, the following codepoint settings are true:

Codepoint	Default Priority
001100	1
001101	No-override
001110	2

If you change all three settings to a priority of 3, and then execute **write memory**, the switch will reflect these changes in the show config listing:

```
ProCurve (config)# qos dscp-map 001100 priority 3
ProCurve (config)# qos dscp-map 001101 priority 3
ProCurve (config)# qos dscp-map 001110 priority 3
ProCurve (config)# write memory
ProCurve (config)# show config

Startup configuration:

; 498358-B21 Configuration Editor; Created on release #Z.14.XX

hostname "ProCurve 6120G/XG Blade Switch"
qos dscp-map 001100 priority 3
qos dscp-map 001101 priority 3
qos dscp-map 001110 priority 3
interface D1
.
.
.
```

Configure these three codepoints with non-default priorities.

Show config lists the non default codepoint settings.

Figure 5-16. Example of Show Config Listing with Non-Default Priority Settings in the DSCP Table

Effect of "No-override". In the QoS Type-of-Service differentiated services mode, a **No-override** assignment for the codepoint of an outbound packet means that QoS is effectively disabled for such packets. That is, QoS does not affect the packet priority or VLAN tagging. In this case, the packets are handled as follows (as long as no other QoS feature creates priority assignments for them):

802.1Q Status	Outbound 802.1p Priority
Received and Forwarded on a tagged port member of a VLAN.	Unchanged
Received on an Untagged port member of a VLAN; Forwarded on a tagged port member of a VLAN.	0 (zero)—"normal"
Forwarded on an Untagged port member of a VLAN.	None

Notes on Changing a Priority Setting

If a QoS classifier is using a policy (codepoint and associated priority) in the DSCP Policy table, you must delete or change this usage before you can change the priority setting on the codepoint. Otherwise the switch blocks the change and displays this message:

```
Cannot modify DSCP Policy < codepoint > - in use by
other qos rules.
```

In this case, use **show qos < *classifier* >** to identify the specific classifiers using the policy you want to change; that is:

```
show qos port-priority
show qos type-of-service
```

For example, suppose that the 000001 codepoint has a priority of 6, and several classifiers use the 000001 codepoint to assign a priority to their respective types of traffic. If you wanted to change the priority of codepoint 000001 you would do the following:

1. Identify which QoS classifiers use the codepoint.
2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to **No-override**.
3. Reconfigure the desired priority for the 000001 codepoint.
4. Either reassign the classifiers to the 00001 codepoint policy or leave them as they were after step 2, above.

Error Messages caused by DSCP Policy Changes

Refer to the following table on ways to fix errors that may be generated when configuring DSCP policy changes.

Message	Meaning
DSCP Policy < ***decimal-codepoint*** > not configured	You have attempted to map a QoS classifier to a codepoint for which there is no configured priority (**No-override**). Use the **qos dscp-map** command to configure a priority for the codepoint, then map the classifier to the codepoint.

Message	Meaning
Cannot modify DSCP Policy < ***codepoint*** > - in use by other qos rules.	You have attempted to map a QoS classifier to a codepoint that is already in use by other QoS classifiers. Before remapping the codepoint to a new priority, you must reconfigure the other QoS classifiers so that they do not use this codepoint. You can have multiple QoS classifiers use this same codepoint as long as it is acceptable for all such classifiers to use the same priority.

Table 5-10. Error Messages Generated by DSCP Policy Changes

Example of Changing the Priority Setting on a Policy When One or More Classifiers Are Currently Using the Policy

Suppose that codepoint 000001 is in use by one or more classifiers. If you try to change its priority, you see a result similar to the following:

```
ProCurve(config)# qos dscp-map 000001 priority 2
Cannot modify DSCP Policy 000001 - in use by other qos rules.
```

Figure 5-17. Example of Trying To Change the Priority on a Policy In Use by a Classifier

In this case, you would use steps similar to the following to change the priority.

1. Identify which classifiers use the codepoint you want to change.

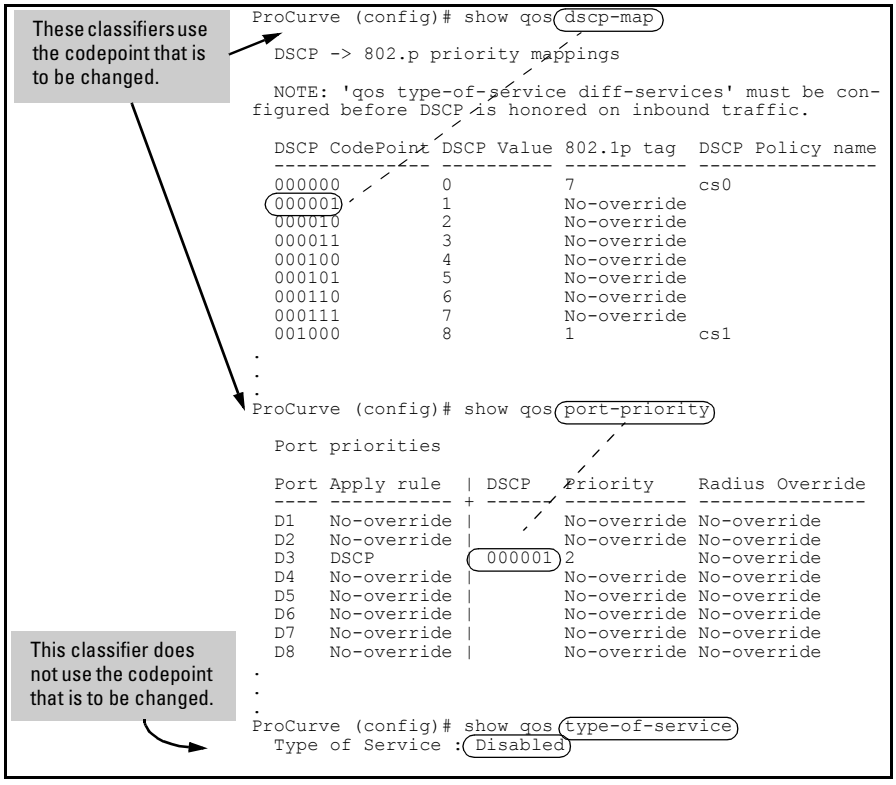

These classifiers use the codepoint that is to be changed.
This classifier does not use the codepoint that is to be changed.
ProCurve (config)# show qos dscp-map
DSCP -> 802.p priority mappings
NOTE: 'qos type-of-service diff-services' must be configured before DSCP is honored on inbound traffic.
DSCP CodePoint DSCP Value 802.1p tag DSCP Policy name
000000 0 7 cs0
000001 1 No-override
000010 2 No-override
000011 3 No-override
000100 4 No-override
000101 5 No-override
000110 6 No-override
000111 7 No-override
001000 8 1 cs1
ProCurve (config)# show qos port-priority
Port priorities
Port Apply rule | DSCP Priority Radius Override
D1 No-override | No-override No-override
D2 No-override | No-override No-override
D3 DSCP 000001 2 No-override
D4 No-override | No-override No-override
D5 No-override | No-override No-override
D6 No-override | No-override No-override
D7 No-override | No-override No-override
D8 No-override | No-override No-override
ProCurve (config)# show qos type-of-service
Type of Service : Disabled

Figure 5-18. Example of a Search to Identify Classifiers Using a Codepoint You Want To Change

2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to **No-override**. For example:
   a. Delete the policy assignment for the **dscp-map** classifier. (That is, assign it to **No-override**.)

      ```
      ProCurve(config)# no qos dscp-map 5
      ```

   b. Create a new DSCP policy to use for re-assigning the remaining classifiers.

      ```
      ProCurve(config)# qos dscp-map 000100 priority 6
      ```

   c. Assign the **port-priority** classifier to the new DSCP policy.

      ```
      ProCurve(config)# int e d1 qos dscp 000100
      ```

3. Reconfigure the desired priority for the 000001 codepoint.

   ```
   ProCurve(config)# qos dscp-map 000001 priority 4
   ```

4. You could now re-assign the classifiers to the original policy codepoint or leave them as currently configured.

QoS Queue Configuration

By default, there are four priority queues or traffic classes. These are shared across all ports. This number cannot be reconfigured.

QoS Operating Notes and Restrictions

QoS support based on packet type is shown below.

Table 5-11. Details of Packet Criteria and Restrictions for QoS Support

Packet Criteria or Restriction	QoS Classifiers				DSCP Overwrite (Re-Marking)
	Device Priority (IP Address)	IP Type-of-Service	Source Port	Incoming 802.1p	
Restricted to IPv4 Packets Only	Yes	Yes	No	No	Yes
Allow Packets with IP Options[1]	Yes	Yes	Yes	Yes	Yes
Support IPv6 Packets[2]	No	No	Yes	Yes	No
Support Layer-2 SAP Encapsulation	No	No	Yes	Yes	No

[1]An "IP Option" is an optional, extra field in the header of an IP packet.
[2]All Switches: For explicit QoS support of IPv6 packets, force IPv6 traffic into its own set of VLANs and then configure VLAN-based classifiers for those VLANs.

- **All Switches:** For explicit QoS support of IP subnets, ProCurve recommends forcing IP subnets onto separate VLANs and then configuring VLAN-based classifiers for those VLANs.
- **For Devices that Do Not Support 802.1Q VLAN-Tagged Ports:** For communication between these devices and the switch, connect the device to a switch port configured as **Untagged** for the VLAN in which you want the device's traffic to move.
- **Port Tagging Rules:** For a port on the switch to be a member of a VLAN, the port must be configured as either **Tagged** or **Untagged** for that VLAN. A port can be an untagged member of only one VLAN of a given protocol type. Otherwise, the switch cannot determine which VLAN should receive untagged traffic. For more on VLANs, refer to chapter 2, "Static Virtual LANs (VLANs)".
- **Maximum QoS Configuration Entries:** The switches covered in this guide accept the maximum outbound priority and/or DSCP policy configuration entries. They support a maximum of 250 QoS entries. Each device (IP address) QoS configuration uses two entries. Each TCP/UDP port QoS configuration uses two entries. All other classifier configurations use one entry each.

Table 5-12. Maximum QoS Entries.

Switch	Software Version	Maximum QoS Entries	Notes
Switch 6120		250*	• Each device (IP address) QoS configuration uses two entries. • Each TCP/UDP port QoS configuration uses two entries. • All other classifier configurations use one entry each.
*Configuring device (IP address) or TCP/UDP QoS entries reduces this maximum. See the "Notes" column.			

Attempting to exceed the above limits generates the following message in the CLI:

```
Unable to add this QoS rule. Maximum number (entry-#)
already reached.
```

- **Not Supported:** Use of an inbound 802.1p packet priority as a classifier for remapping a packet's outbound priority to different 802.1p priority. For example, where inbound packets carry an 802.1p priority of 1, QoS cannot be configured use this priority as a classifier for changing the outbound priority to 0.
- **Monitoring Shared Resources:** The QoS feature shares internal switch resources with several other features. The switch provides ample resources for all features. However, if the internal resources become fully subscribed, additional QoS provisions cannot be configured until the necessary resources are released from other uses. For information on determining the current resource availability and usage, refer to the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.

IP Multicast (IGMP) Interaction with QoS

IGMP high-priority-forward causes the switch to service the subscribed IP multicast group traffic at high priority, even if QoS on the switch has relegated the traffic to a lower priority. This does not affect any QoS priority settings, so the QoS priority is honored by downstream devices. However, QoS does take precedence over IGMP normal-priority traffic.

The switch's ability to prioritize IGMP traffic for either a normal or high priority outbound queue overrides any QoS criteria, and does not affect any 802.1p priority settings the switch may assign. For a given packet, if both IGMP high priority and QoS are configured, the QoS classification occurs and the switch marks the packet for downstream devices, but the packet is serviced by the high-priority queue when leaving the switch.

IGMP High Priority	QoS Configuration Affects Packet	Switch Port Output Queue	Outbound 802.1p Setting (Requires Tagged VLAN)
Not Enabled	Yes	Determined by QoS	Determined by QoS
Enabled	See above paragraph.	High	As determined by QoS if QoS is active.

Index

Numerics

802.1p priority (QoS)
definition … 5-6
802.1Q VLAN tagging … 3-3
802.1w as a region … 4-16

A

advertisement, GVRP
definition … 3-3

B

bandwidth
effect of QoS … 5-1
bandwidth loss, spanning tree … 4-12
blocked link from STP operation … 4-12
blocked port
from STP operation … 4-10
Bootp
gateway ignored … 2-46
BPDU … 3-3
BPDU port protection
See spanning-tree, 802.1s.
bridge protocol data unit … 3-3
broadcast domain … 2-4
broadcast storm … 4-3

C

command syntax conventions … 1-2
configuration … 4-10
Class of Service … 5-11
factory default … 2-21, 2-27, 4-9
spanning tree protocol … 4-10

D

dedicated management VLAN … 2-45
default settings
GVRP unknown VLAN, *learn* … 3-8
GVRP, *disabled* … 3-3
loop protection, *disabled* … 4-71
management VLAN, *disabled* … 2-49
MSTP … 4-3
default settings recommended … 4-6, 4-9
MST instance, *0* … 4-66
See also spanning tree. … 4-3
QoS … 5-3
codepoint priority settings … 5-34
qos port queues, *8* … 5-9
qos tos ip precedence, *disabled* … 5-16
spanning tree … 4-3
config-name … 4-21
config-revision, *0* … 4-22
forward-delay, *15* … 4-23
hello-time, *2* … 4-23
max-hops, *20* … 4-19, 4-23
maximum age, *20* … 4-23
path cost values … 4-17
per port parameters … 4-26–4-30
spanning tree operation, *off* … 4-9
static VLANs, *8* … 2-4
VLAN name … 2-28, 2-35
VLAN support, *256 VLANs* … 2-16
default VLAN … 2-9, 2-13, 2-27, 2-45
DHCP
gateway ignored … 2-46
documentation
feature matrix … -x
latest versions … -ix
printed in-box publication … -ix
release notes … -ix
downstream device (QoS)
definition … 5-6
effect of priority settings … 5-9
DSCP
Policy Table … 5-34
policy, defined … 5-6
See also priority.

F

forbid option
See GVRP.
forwarding database
See VLAN.

G

GARP
See GVRP.
gateway
manual config priority … 2-46
GVRP … 4-8
advertisement … 3-19
advertisement, defined … 3-3
advertisement, responses to … 3-6
advertisements, generating … 3-11
auto option … 3-10
benefit … 3-3
block … 3-8
CLI, configuring … 3-14
configurable port options … 3-6
configuring learn, block, disable … 3-8
convert dynamic to static … 3-7
converting to static VLAN … 3-3
disable … 3-8
dynamic VLAN and reboots … 3-19
dynamic VLANs always tagged … 3-4
forbid option … 3-10
GARP … 3-3
general operation … 3-4
IP addressing … 3-7
jumbo frames … 3-19
learn … 3-8
learn, block, disable … 3-10
menu, configuring … 3-13
non-GVRP aware … 3-18
non-GVRP device … 3-18
operating notes … 3-18
port control options … 3-11
port-leave from dynamic … 3-11
reboot, switch … 3-12
recommended tagging … 3-11
standard … 3-3
tagged, dynamic VLAN … 3-4
unknown VLAN … 3-11
unknown VLAN, options … 3-7
VLAN behavior … 2-12
VLAN, dynamic adds … 2-25
VLAN, maximum … 3-18

H

Help
for CLI … 1-7
for menu interface … 1-6
for web browser interface … 1-7

I

inbound port (QoS)
definition … 5-6
IP
gateway … 2-46
traffic priority based on ToS field … 5-15
IP address
quick start … 1-8
IP, type of service
configuring priority … 5-15
IPv6
management VLAN is for v6 traffic … 2-53

J

jumbo frames
GVRP … 3-19

L

legacy VLAN … 2-11
loop protection
configuring … 4-70
send-disable … 4-70
show … 4-72
transmit-interval … 4-71
trap … 4-71
used for unmanaged devices … 4-3
loop, network … 4-10

M

MAC address
duplicate … 2-17
per switch … 2-17
per VLAN … 2-17
same for all VLANs … 2-56
single forwarding database … 2-17
management VLAN, secure
See secure management VLAN
maximum VLANs, GVRP … 3-18
mesh
management VLAN … 2-53
spanning tree … 4-16

message
VLAN already exists … 2-38
MSTI, configuration … 4-35
MSTP
instance mapping … 4-43
preconfigure benefits … 4-42
preconfigure topology … 4-42
preconfigure vlans in instance … 4-43
saving current configuration … 4-47
See spanning-tree, 802.1s.
vlan range option … 4-44
multiple forwarding database … 2-17

N

non-routable VLAN … 2-53

O

outbound port (QoS)
definition … 5-6
outbound port queue (QoS)
definition … 5-7

P

path costs
802.1D STP versus RSTP and MSTP … 4-17
configuring 802.1D STP pathcost values … 4-23
port
blocked by STP operation … 4-10
loop … 4-10
monitoring … 2-56
redundant path … 4-10
port trunk
VLAN … 2-56
precedence bits (QoS)
definition … 5-6
primary VLAN
See VLAN, primary.
priority
802.1p priority, defined … 5-6
codepoint, defined … 5-6
downstream device, defined … 5-6
DSCP policy, defined … 5-6
DSCP, defined … 5-6
inbound port, defined … 5-6
outbound port, defined … 5-6
upstream device, defined … 5-7
priority (QoS)
criteria for prioritizing packets … 5-10
type of service screen … 5-15
VLAN ID priority … 5-27
ProCurve
switch documentation … -ix

Q

Quality of Service
basic operation … 5-7
configuring … 5-11, 5-14
configuring IP type of service … 5-15
criteria for prioritizing outbound packets … 5-10
definitions of terms … 5-6
DSCP Policy Table … 5-34
maximum entry limit … 5-41
no override definition … 5-13
No override, effect of … 5-35
overview … 5-1
prioritizing traffic based on IP ToS field … 5-15
priority settings map to outbound queues … 5-9
priority settings mapped to downstream devices … 5-9
type of service screen … 5-15
VLAN ID priority … 5-27
Quick Installation Card … 1-4
quick start … 1-8

R

redundant path … 4-10
region … 4-10
See spanning-tree, 802.1s.
revision number … 4-14
root-history … 4-58
routing
non-routable VLAN … 2-53

S

secure management VLAN … 2-46
setup screen … 1-8
single forwarding database … 2-17
spanning tree
802.1s
See spanning tree, 802.1s.

blocked link … 4-12
blocked port … 4-10
broadcast storm … 4-3
enabling MSTP … 4-40
MSTP
See spanning-tree, 802.1s
VLAN effect on … 2-55
spanning-tree
config-name … 4-43
config-revision … 4-43
instance vlan … 4-42, 4-43
root-history … 4-58
spanning-tree, 802.1s … 4-4, 4-6
802.1D and 802.1w connections … 4-16
802.1D as a region … 4-13, 4-16
802.1Q VLANs … 4-12
802.1s standard-compliant … 4-6
802.1w as a region … 4-13
active path … 4-10
active paths … 4-15
bandwidth loss … 4-12
benefit … 4-6
blocked traffic … 4-11
boundary port, region … 4-14, 4-15
boundary port, VLAN membership … 4-11
BPDU … 4-11, 4-19, 4-22, 4-23, 4-27
BPDU requirement … 4-14
BPDU, function … 4-14
bridge … 4-14
bridge, designated for region … 4-14
caution … 4-6, 4-9
CIST … 4-8, 4-13, 4-15
CIST per-port hello time … 4-15
CIST root … 4-27
CIST root, display change history … 4-58
common and internal spanning tree
See CIST.
common spanning tree
See CST.
compatibility … 4-16
compatibility mode … 4-22
configuration … 4-21, 4-40
configuration identifier … 4-14
configuration steps … 4-19
configuration, BPDU port protection … 4-30
configuration, exchanging … 4-40
configuration, MST instance … 4-35
configuration, MSTI per-port … 4-37
configuration, port … 4-26
CST … 4-8, 4-11, 4-13
CST and legacy devices … 4-11
CST, view status … 4-51, 4-52
debug, display counters … 4-61, 4-62, 4-64
default configuration … 4-9
designated bridge … 4-11, 4-14
designated port … 4-11
disabling MSTP … 4-40
display statistics and configuration … 4-49
dynamic VLANs, disallowed … 4-9
edge port … 4-26
enabling a region … 4-40
enabling MSTP … 4-40
example of multiple topologies … 4-10
fault tolerance … 4-6
force protocol version … 4-16
forward-delay … 4-23
forwarding paths … 4-16
forwarding state … 4-26
frame duplication and misordering … 4-16
general operation … 4-4, 4-6
GVRP … 4-8, 4-15
hello-time, CIST root, propagated … 4-15, 4-23
hello-time, override … 4-15
hello-time, propagated … 4-15
hop-count decremented … 4-23
instance … 4-4, 4-15, 4-20
instance, display debug counters … 4-61, 4-62, 4-64
instance, forwarding topology … 4-16
instance, IST … 4-8
instance, type … 4-8
internal spanning tree
See IST.
interoperating with 802.1D and 802.1w … 4-13
IST … 4-8
IST instance … 4-8, 4-35, 4-44
IST root … 4-8, 4-10, 4-14
IST root, display change history … 4-58
IST, defined … 4-13
IST, dynamic VLAN … 4-15
IST, root switch … 4-13
IST, switch membership … 4-13
IST, VLAN membership … 4-8
legacy devices and the CST … 4-11
legacy STP and RSTP … 4-11
mesh environment … 4-6, 4-16

MIB … 4-49
MST region
See region.
MSTI … 4-8, 4-15
MSTI root … 4-10
MSTI root, display change history … 4-58
MSTI, view status … 4-53
MSTP … 4-9
MSTP operation … 4-9
MSTP, view global configuration … 4-54
multiple spanning tree instance
See MSTI
override hello-time … 4-15
path cost, effect on 802.1D … 4-16
pending configuration … 4-57
pending option … 4-9, 4-22, 4-40
per-VLAN STP … 4-6
planning … 4-17
port connectivity … 4-26
port states … 4-10, 4-16
priority resolution … 4-36
priority, device … 4-19, 4-25
priority, IST port … 4-39
priority, MSTI port … 4-38
rapid state transitions … 4-16
redundant links … 4-11
region … 4-4, 4-7, 4-8, 4-9
region name … 4-14, 4-21
region root switch … 4-8
region, configuration name … 4-69
region, Configuration Revision number … 4-69
region, defined … 4-14
region, enabling … 4-40
region, root bridge … 4-13
region, RSTP bridge … 4-15
region, switch configuration … 4-15
region, switch excluded … 4-69
region, view configuration … 4-56
region, VLAN assignments … 4-14
regional boundary port … 4-14
regional root bridge per-instance … 4-11
regional root switch … 4-13
regional root switch, configuration … 4-15
regions, communication between … 4-15
root bridge … 4-8
root bridge per-instance … 4-11
root bridge per-region … 4-13
root port per-instance … 4-11
root switch, instance … 4-36
root switch, IST instance … 4-8, 4-13
root switch, MST instance … 4-15
root switch, regional … 4-13
root, CIST … 4-23
root, IST … 4-14
root, MSTI … 4-10
routed traffic in a region … 4-11
RSTP as a region … 4-7
RSTP BPDU requirement … 4-14
RSTP bridge … 4-15
rules for operation … 4-15
separate forwarding paths … 4-8
show commands … 4-49, 4-58
SNMP MIB … 4-49
STP as a region … 4-7
switch excluded from region … 4-69
topology between regions … 4-10
troubleshooting … 4-58
trunk, root, per-instance … 4-11
trunked link … 4-54
trunked link example … 4-12
types of MST instances … 4-8
VLAN assignments, region … 4-14, 4-15
VLAN membership, region … 4-12
VLAN, change instance … 4-20
VLAN, configuration error … 4-69
VLAN, connectivity between regions … 4-15
VLAN, duplicate or missing packets … 4-69
VLAN, dynamic … 4-8
VLAN, instance assigned … 4-10, 4-15, 4-35, 4-44
with legacy STP and RSTP … 4-7
static VLAN, convert to … 3-3
subnet address … 2-7

T

ToS
See Type of Service.
trunk, spanning-tree example … 4-12
Type of Service
configuring packet priority … 5-15
how the switch uses ToS configuration … 5-26
using to prioritize IP traffic … 5-15

U

upstream device (QoS)

definition … 5-7

V

VID
See VLAN.
VLAN
already exists, message … 2-38
broadcast domain … 2-4
CLI, commands … 2-28
CLI, configuring parameters … 2-27
convert dynamic to static … 2-37, 3-3
dedicated management … 2-45
default VLAN VID … 2-45
default VLAN, name change … 2-45
DEFAULT_ VLAN … 2-45
deleting … 2-14, 2-35, 2-57
deleting, with member ports … 2-14, 2-35, 2-36
DHCP, primary VLAN … 2-45
duplicate MAC address … 2-17
dynamic … 2-4, 2-16, 2-21, 2-27, 2-37, 4-15
effect on spanning tree … 2-55
gateway, IP … 2-46
GVRP, auto … 2-13
IP interface relationship … 2-56
layer-2 broadcast domain … 2-5
layer-3 broadcast domain … 2-5
limit … 2-21, 2-27
MAC address assignment … 2-56
maximum, GVRP … 3-18
menu, configuring parameters … 2-21
menu, maximum capacity … 2-25
menu, missing VLAN … 2-25
multiple forwarding database … 2-17, 2-20
multiple VLANs on port … 2-42
non-routable … 2-53
number allowed, including dynamic … 2-25
per port configuration options … 2-12
port assignment … 2-25
port configuration … 2-44
port monitoring … 2-56
port restriction … 2-57
port trunk … 2-56
port-based … 2-5
primary … 2-34, 2-45
primary, CLI command … 2-28, 2-34
primary, select in menu … 2-22
primary, web configure … 2-39
primary, with DHCP … 2-13
prioritizing traffic from with QoS … 5-27
protocol … 2-5, 2-6, 2-10, 2-13, 2-15, 2-56
ARP requirement … 2-13, 2-35
capacity per VLAN … 2-13
CLI only … 2-21
commands … 2-28
compared to port-based … 2-7
configuration … 2-27, 2-35
example … 2-43
forbid option not allowed … 2-38
IP addressing … 2-7
IPv4, ARP requirement … 2-13, 2-35
IPv6 … 2-7
limit … 2-12
limit on types per-port … 2-7
non-routable … 2-40
operation … 2-15
port membership limit … 2-7
primary VLAN not allowed … 2-34, 2-46
router, external … 2-8
routing … 2-5, 2-8
status … 2-29, 2-30, 2-32
tagged … 2-12, 2-42
tagged member … 2-8
tagging … 2-8
traffic separation … 2-4
types … 2-35
untagged member … 2-7
untagged packet forwarding … 2-14
untagged, limit … 2-12
untagged, multiple … 2-42
untagged, restriction … 2-57
restrictions … 2-57
routing between VLANs … 2-4
routing, protocol VLANs … 2-5
secure management … 2-46
security, network … 2-4
show vlan ports detail … 2-29
single forwarding database … 2-17
static … 2-4, 2-6, 2-21, 2-27, 2-46
subnet … 2-4
switch capacity … 2-4
tagging … 2-40, 2-42
unknown VLAN … 3-11
untagged … 2-11, 2-26
untagged, operation … 2-15
VID … 2-4, 2-42

VID, default VLAN … 2-45
voice … 2-5, 2-29, 2-30, 2-32, 2-55
voice, configuration … 2-36
voice, configuring … 2-28
voice, VLAN type … 2-13
web browser configuration … 2-39
See also GVRP.
VLANs
static, 802.1s spanning tree … 4-8
voice VLAN
See VLAN.
VoIP
operating rules … 2-13
See also VLAN, voice.

W

warranty … -i
web browser interface
configuring VLANs … 2-39
write memory
converting dynamic to static VLAN … 3-18

Technology for better business outcomes

To learn more, visit
www.hp.com/go/bladesystem/documentation/

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.

August 2009

Manual Part Number
5992-5524